XpanDH

Expanding Digital Health through a pan-European EHRxF-based Ecosystem

D1.7 – (D1.5.2) – EEHRxF legal, cybersecurity & trust issues Report

WP1 – Coordination

21.07. 2023

Authors:

Name	Organisation	Name	Organisation
Petra Wilson	IHE		
Anderson Carmo	ISCTE		
Alberto Zanini	ARIA		
Evangelos Markatos	FORTH		

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HaDEA. Neither the European Union nor the granting authority can be held responsible for them.

Document control	
Status	Draft
Version	0.1
Type of Document	R: Document, report;
Dissemination Level	PU – Public
Work Package	WP1 – Coordination
Full document name	D1.7 – (D1.5.2) – EEHRxF legal, cybersecurity & trust issues Report
Link to access document	N/A
Partner lead(s)	ISCTE
Other partners involved	HL-7, EMP, IHE- EUR, UNINOVA, ECHA, I~HD
What did this document aim to achieve?	The aim of this document is to present to the consortium partners the basic concepts and rules that will be implemented on the project.
Present the main methodological approaches in bullet point format	
What were the main findings or take-away messages? What implications does it have for the XpanDH project?	
Which project stakeholder group would benefit the most from the document and why?	

Healthcare Professional	
International Adherence Network/Initiative	
Investors and Funding	
Patient Organization	Yes
Patient/Caregiver	
Pharma (Marketing & Sales / Medical Dept./ R&D)	
Public Authority or Policymaker	
Regulatory body	
Standardization Body/ Open-Source Network Researcher/Academic	
Statutory Health Insurance Company	
Technology & Service Provider	
Other	

List any relevant organizations or social media accounts for wider visibility	

Revision History			
Version	**Date**	**Author**	**Description**
0.1	20/06/2023	Petra Wilson	1st document outline
0.2	30/06/2023	Petra Wilson	1st full draft
0.3	15/07/2023	Alberto Zanini; Evangelos Markatos	First Review
0.4	20/07/2023	Petra Wilson	Updated of the deliverable content accordingly the comments received.
1.0	21/07/2023	Anderson Carmo	Final revision on the document prior EC submission.

Table of Contents

Table of Figures

List of abbreviations

Acronym	Description
AI	artificial intelligence
AI Act	Artificial Intelligence Act
B2B	Business to Business
B2C	Business to Consumer
B2G	Business to Government
CRA	Cyber Resilience Act
CSA	Cybersecurity Act
CSIRT	Computer Security Incident Response Team
DPIA	Data Protection Impact Assessment
EEHRxF	European Electronic Health Records Exchange Format
EHDS	European Health Data Space
eHDSI	eHealth Digital Services Infrastructure
EHR	electronic Health Record
eID	electronic identification
eIDAS	Electronic Identification and Trust Service Regulation
ENISA	EU Agency for Network and Information Security
EU	European Union
FAIR	Findable, Accessible, Interoperable, Reusable
GDPR	General Data Protection Regulation
ICT	Information and Communications Technology
IVDR	In Vitro Diagnostic Medical Devices Regulation
MDR	Medical Device Regulation
NIS2	Network and Information Security 2 Directive
RAPEX	Rapid Exchange of Information System
RRF	EU Recovery and Resilience Facility
SaMD	Software as a Medical Device
SME	Small and medium-sized enterprises
TFEU	Functioning of the European Union
UDI	Unique Device Identifier
VPN	Virtual Private Network

Executive summary

This is the first iteration of a document which seeks to provide a high-level overview of a wide range of EU level legislation which impacts the adoption and use of digital health solutions.

It is divided into three sections looking at the overarching EU legal principle of ensuring **access to healthcare** for all persons, as enshrined in the European Convention of Human Rights and the Treaty on the Functioning of the European Union (TFEU). It then looks at how these are balanced with two other overarching legal principles: **the establishment of the EU internal market** and **respect for data protection** in national and EU law. From looking at high level principles it considers how key EU level legislation impacts the use of digital health solutions within and across EU borders.

The objective is to demonstrate the range of competing issues that must be borne in mind when addressing the legal aspects of implementing digital health solutions and to provide a general reference on legal issues which must be addressed. The issues raised under the pillars on access to care and internal market will be addressed in a high-level overview manner. However, more detailed coverage is given to the pillar on data protection as this is central to the focus of XpanDH, with a particular focus on General Data Protection Regulation (GDPR) in this iteration of this document with more detailed guidance on digital security to be addressed in the second iteration of this document, as will specific measures under the European Health Data Space Regulation and Data Act as these become more stable in the negotiations between the European Commission, Parliament and Council.

Given that European Health Data Space (EHDS) and key data security legislation is still in negotiation, a second iteration of this document will be developed later in the project's lifetime, when the legislation is more stable, but also when the work undertaken in the XpanDH bubbles will have identified the needs of digital health stakeholders more clearly.

1 Introduction

1.1 Background

XpanDH is designed to build capacity in individuals and organisations to create, adapt and explore purposeful use of interoperable digital health solutions based on a shared adoption of the European Electronic Health Records Exchange format (EEHRxF) across Europe. It seeks to develop networks among stakeholder and experts in the field and to support them with tailored guidance and real examples to help them advance in the use of EEHRxF-embedded digital health solutions to add value to health and care and promote Personal and European Health Data Spaces.

A key aspect of developing the confidence of potential users of digital health tools within their healthcare systems is to help them better understand the legal and ethical frameworks within which they are obliged to operate. The applicable legal requirements for any given healthcare provider organisation will need to be addressed *in situ* with the local parties holding legal responsibility. Such parties will usually include the Chief Executive Officer, Chief Medical and Nursing Officer, Chief Informatics Officer, General Council and the Data Protection Officer of the organisation; as well as officers at local authority level. Despite the need for local knowledge and adaptation, a core range of legal issues will arise in all healthcare settings, which are addressed also at European Union (EU) level.

1.2 Scope and objectives

The purpose of the present document is to provide an overview of the EU level law and policy which must be considered at when digital health implementation decisions are being made in EU Member States. The document does not purport to provide answers to all possible questions, but it seeks to provide stakeholders with a baseline of knowledge which will help them pursue the issues at local level with the relevant responsible parties.

The document begins by exploring overarching EU and national level legal principle of ensuring **access to healthcare** for all persons, as enshrined in the European Convention of Human Rights and the Treaty on the Functioning of the European Union (TFEU). It then looks at how these are balanced with two other overarching legal principles: **the establishment of the EU internal market** and **respect for data protection** in national and EU law. From looking at high level principles it considers how key EU level legislation impacts the use of digital health solutions within and across EU borders.

The exploration of a wide range of legislation under the three-pillars of equitable access, internal market and data protection provides the project partners with an overview of key EU level legislation which will have an impact on how digital health

solutions are implemented. The legislation covered is not an exhaustive list, but rather a selection of legislation which most directly impacts digital health given that there is no single EU legislative act on digital health.

This document is designed to demonstrate the range of competing issues that must be borne in mind when addressing the legal aspects of implementing digital health solutions and to provide a general reference on legal issues which must be addressed. The issues raised under the pillars on access to care and internal market will be addressed in a high-level overview manner. However, more detailed coverage is given to the pillar on data protection as this is central to the focus of XpanDH, with a particular focus on GDPR in this iteration of this document with more detailed guidance on digital security to be addressed in the second iteration of this document, as will specific measures under the European Health Data Space Regulation and Data Act as these become more stable in the negotiations between the European Commission, Parliament and Council.

The project XpanDH aims at mobilizing and building capacity in individuals and organisations to create, adapt and explore purposeful use of interoperable digital health solutions based on a shared adoption of the European Electronic Health Records Exchange format across Europe.

To achieve this main goal, the project is considering the outputs and outcomes of past projects, such as X-eHealth, to develop the specifications to be used on the adoption domains, and further feasibility evaluation, implementation and testing among the project partners and stakeholders.

2 The EU legal landscape for digital health solutions implementation

The EU legal landscape within which digital health solutions exist may be seen as straddling three broad areas of EU legislation, which will at times be in competition with one another.

Access to healthcare - the role of the EU is to complement the Member State or regional level actions in providing healthcare. Strictly speaking the EU does not have a direct legal competence (the right to enact legislation) in the area of healthcare provision. Accordingly, EU level legislation which impacts the delivery of healthcare must carefully balance the role of the EU with that of the Member State.

The internal market – a core function of the EU is to build the internal market which the EU recognises through the principles of the freedom of movement of workers, services, goods and capital. These values necessarily touch upon the freedom of movement of healthcare professionals to provide services and patient to use services; as well as industry to bring products to market across the EU on a level playing field.

Data protection – the EU recognises that everyone has the right to the protection of personal data concerning them, accordingly EU level legislation has been enacted on data protection. This however must be balanced with the need to allow data to flow and be shared for the purposes of allowing safe and equitable access to healthcare as well as allowing the internal market in digital health goods and services to flourish.

Several scholars[1, 2, 3]in EU health policy have noted a tri-fold dimension to EU health policy, it should be noted however that when this is applied to health policy more generally, rather than policy which impacts the use of digital solutions, a major focus is on fiscal governance as a pillar in its own right, while data protection is included under internal market. We have chosen in this presentation of EU policy relating to digital health to discuss fiscal governance only briefly, and to focus in more detail on data protection as a core pillar of digital health policy at EU level.

The graphic overleaf shows the broad range of legislation and policy which is found under the three pillars. It is designed to provide an overview and is not exhaustive. Some legislation has not been included because although it impacts on digital health, it is so broad that to discuss it would distract from the objective of looking at how the uptake of interoperable digital health solutions can be supported. An example of this would be the Working Time Directive (Directive 93/104/EC) which significantly impacts the way in which healthcare systems are organised[4], but is not greatly affected by the adoption of digital solutions. It should also be noted that the allocation of a given piece of legislation under one pillar is not absolute, indeed some pieces of legislation by definition fall under all three. A perfect example of this is the proposed European Health Data Space Regulation, which has been developed to support the internal market (Article 114); protect the interests of individuals in health data concerning them (Article 16) and allow Member States to better co-operate to provide safe healthcare systems (Article 168).

---

[1] Greer SL (2014). The Three Faces of European Union Health Policy: Policy, Markets and Austerity. Policy
and Society, 33:13–24; Palm W & Wismar M (2018). EU integration and health policy at the cross-roads.
Eurohealth, 24(2):19–22

[2] De Ruijter A (2019). EU Health Law & Policy: The Expansion of EU Power in Public Health and Health
Care. Oxford University Press

[3] Scott L. Greer, Sarah Rozenblum, Nick Fahy, Eleanor Brooks, Holly Jarman, Anniek de Ruijter, Willy Palm, Matthias Wismar (2022) Everything you always wanted to know about European Union health policies but were afraid to ask; Third, revised edition

[4] Mossialos E et al. (eds) (2010). Health systems governance in Europe: the role of EU law and policy. Cambridge: Cambridge University Press

As not all the legislation included in the graphic is directly applicable to the scope of XpanDH the sections which follow focus mainly on the legislation which impacts the promotion and adoption of interoperable digital health solutions in a cross border and cross market context. It does not therefore look closely at the legislation on services of general economic interest or on the legislation which supports the freedom of movement, as this is broad ranging legislation which impacts a wide range of products and services and will be applied to digital health solutions in line with its general implementation in Member States. Furthermore, areas of legislation such as these will often have quite significant Member State variation and will therefore need to be considered with specific market settings.

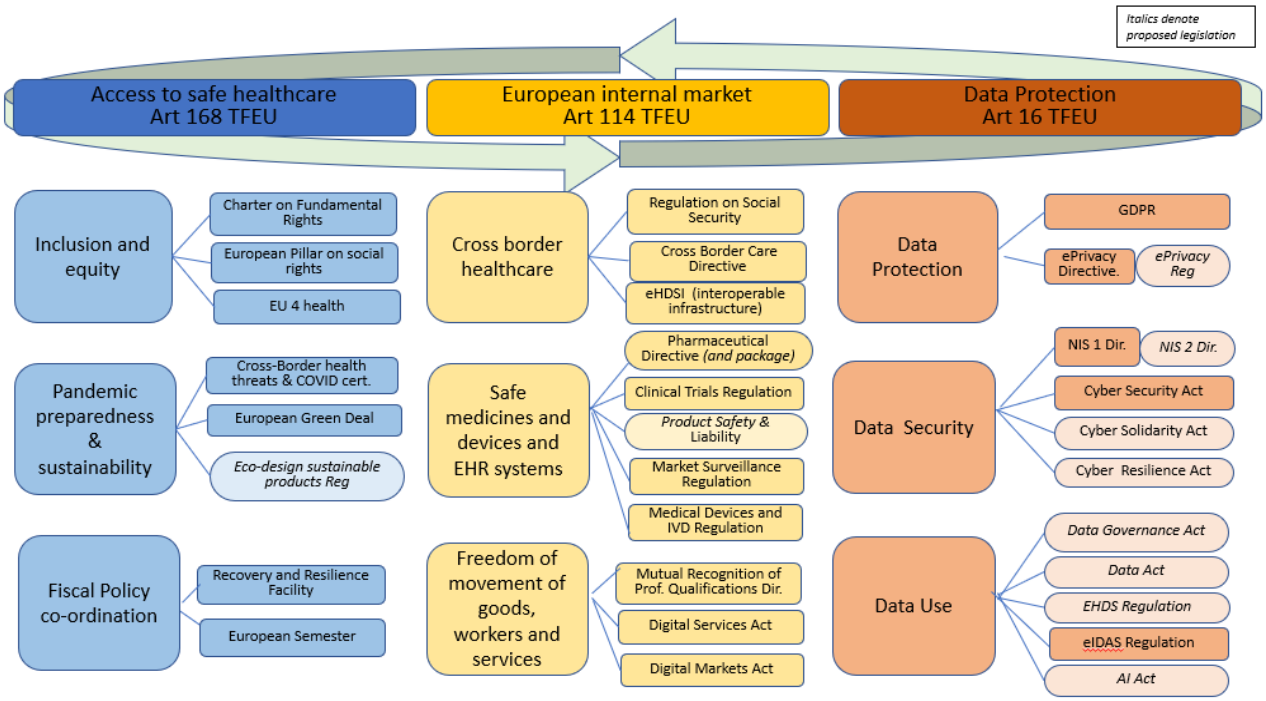

Figure 1: EU Legal Landscape for deployment of digital health solutions

3 Access to healthcare

European citizens have a general right to equitable access to safe healthcare. The way in which this is organised in terms of social insurance systems varies between the Member States, as does the basket of healthcare services available to a citizen in the Member State in which they are insured. The exercise of this right is a complex balance between international human rights law, European law and policy and national law. The discussion of access to healthcare in this document focuses only on the extent to which it is supported by EU level law and policy, which includes, but is not limited to, the law and policy listed in the left side column of Figure 1 above.

The legislation and policy are grouped under three broad headings which encompass the commitment to **inclusion and equity,** the need to ensure **pandemic preparedness sustainable development**, and the **general fiscal policy co-ordination** across the EU. These three groups of EU commitments are derived from the spirit of Article 35 of the **European Charter on Fundamental Rights** and Article 168 of the **Treaty on the Functioning of the European Union (TFEU)** rather than specifically named in those founding laws. Article 35 European Charter on Fundamental Rights states that "Everyone has the right of access to preventive health care and the right to benefit from medical treatment under the conditions established by national laws and practices. A high level of human health protection shall be ensured in the definition and implementation of all Union policies and activities." These principles are echoed in **Article 168 TFEU**, which mandates that "a high level of human health protection shall be ensured in the definition and implementation of all Union policies and activities".

However, Article 168 also clearly states that Union action shall "complement national policies" and that "Member States shall, in liaison with the Commission, coordinate among themselves their policies and programmes, in policies which shall be directed towards improving public health, preventing physical and mental illness and diseases, and obviating sources of danger to physical and mental health. Such action shall cover the fight against the major health scourges, by promoting research into their causes, their transmission and their prevention, as well as health information and education, and monitoring, early warning of and combating serious cross-border threats to health".

Despite the allocation to the EU of a complementing rather than legislating role, known as the principle of subsidiarity, Article 168 provides an exception to this rule in paragraph (4) which allow for the adoption of EU level legislation to ensure "high standards of quality and safety of organs and substances of human origin, blood and blood derivatives" and "measures in the veterinary and phytosanitary fields which have as their direct objective the protection of public health"; and "measures setting high standards of quality and safety for medicinal products and devices for medical use." Furthermore paragraph (5) allows for the adoption of EU level "incentive measures designed to protect and improve human health and in particular to

combat the major cross-border health scourges, measures concerning monitoring, early warning of and combating serious cross-border threats to health, and measures which have as their direct objective the protection of public health regarding tobacco and the abuse of alcohol, excluding any harmonisation of the laws and regulations of the Member States."

Taken as a whole therefore Article 168 ensures that most health-related legislation is developed at national level, which applies as a general rule also to the implementation of digital health solutions within the health systems of each Member State. However, as the remainder of this document makes clear, as healthcare involves the use of products, devices and services that are provided on the European Market to people who are free to provide and consume services across borders, the notion that there is little EU level legislation that impacts on healthcare is misleading.

3.1 Inclusion and Equity

In addition to specific legislation adopted pursuant to the European Charter on Fundamental Rights and the TFEU, the EU's commitment to social inclusion and equity is based in EU policy rather than hard law, and derives in part from the wider policy that has been developed by the Commission since the creation of the European Economic Community. Central to this is the **European Pillar of Social Rights** adopted in 2017 which sets out twenty key principles and rights to support convergence towards better living and working conditions. These are divided into three categories: (i) equal opportunities and access to the labour market, (ii) fair working conditions, and (iii) social protection and inclusion. It is under the latter that a number of health-related policies have been adopted. The commitment is strengthened through targeted financial instruments such as **EU4Health,** which was adopted in 2021 in response to the challenges raised by the COVID Pandemic and Health is an investment and, with a €5.3 billion budget during the 2021-27 period, the EU4Health programme is marks a significant leap forward in EU financial support in the health area and provides "a clear message that public health is a priority for the EU and it is one of the main instruments to pave the way to a European Health Union" as stated on the Commission website for the EU4Health programme. ion"

3.2 Pandemic preparedness and sustainability

The COVID pandemic has viciously underlined the fragility of European health systems in a number of ways, including access to new medicines (vaccines) and basic supplies (personal protective equipment). It also demonstrated the urgent need to recruit and retain healthcare professionals and to co-operate across borders in a much more timely and interoperable manner. The pandemic sped up initiatives that were already in train and demonstrated new ways of working including the Joint Procurement Agreement which allowed Member States to work together in

procuring vaccines and aimed to ensure equitable access to vaccines for all EU countries, to avoid competition between member states, and leverage collective bargaining power to secure favourable prices. It was an emergency response based on legislation from 20135 which allowed for EU level action in the case of serious cross-border health threats, and which has now been replaced by Regulation (EU)2022/2371 on serious cross-border threats to health. The pandemic also drove much closer coordination and collaboration at EU level on health[6], including in digital tools, with the development of a platform to track and trace the **EU COVID-19 digital certificate**, which has provided a significant step in driving digital health interoperability at EU level. Here's how the EU is working on achieving interoperability for the Digital COVID Certificate. It allowed for the development of a common framework for the technical specifications of the Digital COVID Certificate, which ensures that the certificates can be uniformly recognized and verified across the EU member states, based on a a standardized data format for the Digital COVID Certificate which ensures that the certificates can be easily read and verified by different systems and devices used in member states. On a technical level the EU implemented the EU Gateway, which enables the verification and exchange of Digital COVID Certificates across Member States and acts as a secure infrastructure for sharing and validating certificate information. Where need the European Commission provides technical support to member states in implementing and integrating the Digital COVID Certificate system, including guidance on technical specifications, data protection, and interoperability aspects. The learning from this emergency response are therefore highly useful to XpanDH in looking at tools to support wider uptake of cross-border ePrescriptions and sharing of images, laboratory reports and discharge letter to support patient care, and where appropriate allow such data to be re-used to research purposes.

The EU pandemic response sits within a wider framework of sustainability, much of which address issues relevant to healthcare, but focussed on more generic issues such reducing greenhouse gases, promoting renewable energy and transitioning to a circular economy. The 2019 **Green Deal** is central to this policy, setting the overarching policy which seeks to make Europe energy neutral by 2050. A number of pieces of legislation in under the Green Deal which is taken forward in specific objectives, some of which have a direct impact on digital health products. One example, among many, is the **Eco-Design for Sustainable Products Regulation**. Whilst this is a general Regulation, it impacts on the design of medical devices and solutions, and could in due course become relevant for digital health solutions design. The wider principles of green policy will of course also impact digital health, insofar as the most energy efficient and ecologically appropriate design and use

[5] Decision No 1082/2013/EU on serious cross-border threats to health
[6] For a fuller discussion see Gallina Sandra. Preparing Europe for future health threats and crises: the European Health Union. Euro Surveill. 2023;28(5) 6

decisions must underpin digital health implementation policy. In the context of the indicators that the European Semester monitors, healthcare expenditure, healthcare outcomes, access to healthcare services, and the efficiency and effectiveness of healthcare systems are included. As digital health services contribute to meeting the targets under these indicators, they will increasingly feature in the assessments.

3.3 Fiscal Policy Co-ordination

The pandemic also paved the way for more engagement from the EU fiscally on matters of health, including digital health, through the **EU Recovery and Resilience Facility (RRF).** This new approach to funding demonstrates well the impact of non-legislative tools healthcare, and in particular digital health, at EU level. The RRF shows a new approach for driving EU level support and convergence of solutions, within a context of Member State level decision making. In the area of digital health, it is notable that most Member States have indicated they will use funds to improve the healthcare infrastructure, including upgrading networks, enhancing internet connectivity, and expanding broadband access; upgrade electronic health records systems based on EU level interoperability frameworks as well as building digital health skills for healthcare professionals and other stakeholders.

Along side developing policy and legislation derived directly from the TFEU, the EU has an important role in goal-setting, coordination and review, in particular with respect to governance, primarily fiscal governance. This is done through the **European Semester**. The European Semester considers healthcare systems and policies within the broader context of member states' economic and social objectives. The European Semester may therefore include healthcare systems within its Country Specific Recommendations, addressing things such as healthcare system reforms, healthcare spending efficiency, access to healthcare services, or addressing specific healthcare challenges.

Since 2020, in part because of the Pandemic but also because the European Semester has grown in recognition, a broader much set of goals have led to more refined policy recommendations on health. Looking at the European Semester report for 2022[7], we see that Digital Health has been included for several countries, notable as a target for the utilisation to funds from the **EU Recovery and Resilience Facility.**

[7] The European Patients' Forum has provided a useful analysis of health in the 2020 European Semester Report at https://www.eu-patient.eu/globalassets/epf-report---health-in-the-european-semester-2022.pdf, as do EuroHealthNet at https://eurohealthnet.eu/publication/health-and-the-european-semester

4 Internal market

Through the TFEU, and its earlier versions, the EU has been given the exclusive right to legislate against anti-competitive behaviour of market actors, and a strong shared competence in Article 114 TFEU to legislate in order to establish a well-functioning internal market. Central to this is the concept of the free movement of goods, services, persons, capital and the right to establishment, which impacts significantly on healthcare are it concerns services provided to people who have a right to move, both to receive and to provide those services. A significant proportion of all EU level legislation uses Article 114 TFEU which mandate the European Parliament and Council to "*adopt the measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market*".

The internal market applies to healthcare goods and services, and therefore necessarily also to the people who provide the services (healthcare professionals) and patients. Greer et al[8] argue that the internal market is the important face of the EU, it undergirds the wide variety of important policies discussed in this document and means that much of the EU's positive effect on health is through regulations grounded in the internal market. While a very broad range of legislation uses Article 114 as the legal basis to establish legislation that impacts healthcare and digital health, in this document we focus on **cross-border care** which addresses freedom of movement to access healthcare services, the importance of the **safety of medicines and medical devices** offered on the internal market and the wider impact of freedom of movement, including the regulation of the **digital services and digital markets.**

4.1 Cross-Border Care

One of the core objectives of the internal market is to allow workers to move freely. This necessarily means they must be able to benefit from social security coverage, including healthcare, in the country in which they reside, even if this might be temporarily. This is supported by the EU laws on social security coordination which ensures that people can cross borders to work and live, temporarily or permanently, without losing access to social security benefits. As Greer et al stress, it does not mean that there is a European system of social security, any more than there is a European health system, but it ensures that if an individual moves to another country for a job, the social security rights that have been built up (including rights to

[8] Scott L. Greer, Sarah Rozenblum, Nick Fahy, Eleanor Brooks, Holly Jarman, Anniek de Ruijter, Willy Palm, Matthias Wismar (2022) Everything you always wanted to know about European Union health policies but were afraid to ask; Third, revised edition

healthcare) move with the person; similarly, if an individual temporarily travels to another EU country for a purpose such as work, study or holiday and there falls ill, they are covered and will be treated by that country's health system.

In the late 1990s a number of cases were brought to the European Court of Justice which tested the extend to which the rules on co-ordination of social security allowed for patient (as opposed to worker) mobility. These resulted in the Cross-Border Care Directive (Directive 2011/24/EU). The Directive provides that patients who are entitled to a particular health service under the statutory healthcare system in their home country (Member State of affiliation), are generally also entitled to be reimbursed if they choose to receive such treatment in another Member State. The Directive applies to care delivered by private or public sector healthcare establishments. The Directive requires that the patient should generally receive the same level of reimbursement as if the treatment had been received in the Member State of affiliation. However, the level of reimbursement can never exceed the actual costs of the healthcare received, even if a higher amount would have been reimbursed if the care had been provided in the Member State of affiliation. The Directive allows Member States to adopt rules that require patients to seek Prior Authorisation for certain types of treatments. Such Prior Authorisation is limited to treatment requiring at least one overnight stay in hospital, or treatment requiring highly specialised or cost-intensive medical equipment or infrastructure. Prior Authorisation may be refused under certain circumstances, of these the most significant is that the requested treatment is not included in the 'basket of care' of the Member State of affiliation. Member States only have the obligation to reimburse cross-border healthcare under the Directive if such healthcare is among the benefits to which the patient is entitled within the Member State of affiliation. In addition, if the patient can be offered the treatment in the Member State of affiliation within a time limit which is medically justifiable, or if particular risks to the patient or the general population have been identified, Prior Authorisation may also be refused.

The benefits provided under the Directive exist in parallel to benefits provided under **Regulation (EC) No 883/2004 on the coordination of social security systems**. In order to understand why patients may choose to apply for care under the Regulations or Directive, it is important to understand the key similarities and differences between them:

- Both the Regulations and the Directive apply to planned and unplanned healthcare.
- Under the Regulation, Prior Authorisation is generally a requirement for receiving planned treatment in another Member State.
- Under the Directive a requirement of Prior Authorisation is not the rule, however the Member State of affiliation may set up a system of Prior Authorisation for certain kinds of cross-border healthcare.
- The Directive covers all providers, including private (non-contracted) providers, while the Regulations do not impose any obligation on the Member

States with regards to treatment given by providers outside the public scheme.,

- Under the Regulation, reimbursement of healthcare received in a Member State which is not the State of affiliation is made in accordance with the legislation and tariffs of the Member State where the treatment takes place.
- Under the Directive, reimbursement is made in accordance with the legislation and tariffs of the Member State of affiliation.
- The Directive requires up-front payment by patients to the foreign healthcare provider, while the Regulation organise reimbursement between competent institutions except co- payment existing in the Member State of treatment.

The points set out above indicate that in practice planned and unplanned care may often be provided more favourably under the Regulation. Accordingly, patients will often choose to receive care in another Member State under the provisions of the Regulations rather than the Directive, because doing so means they do not have to make an up-front payment and then claim a reimbursement afterwards.

The Regulation makes no provision for care provided by means of digital health. The Directive however envisages the role of digital solutions in two key ways: first, it creates an informal advisory committee to the European Commission on digital health, known as the **eHealth Network**; and secondly it created the first EU level digital health provision through the **European Reference Networks for Rare Diseases**. It also provides the legal basis for the cross-border recognition of prescriptions. The Directive on Cross Border Care is therefore the baseline legislation for digital health at EU level in force in 2023, although this will be supplemented by the **European Health Data Space Regulation** once this is adopted and implemented.

The eHealth Network created by Article 14 of the Cross-Border Care Directive has been instrumental in taking forward the development of digital health in Europe, including in the development of the **European Electronic Health Records Exchange format** which the XpanDH project seeks to support. Recognising that as people move around Europe, whether expressly to receive planned care, or because they are temporarily in another country and require care in an emergency, their care will be safer and more efficient if healthcare professionals have access to their pre-existing medical records, and also if they are able to travel with prescriptions issued in one country that may be dispensed in another. It is in this context that the **eHealth Digital Services Infrastructure (eHDSI)** has been adopted to facilitate the secure exchange of health data across EU Member States, notably by supporting the interoperability of electronic Health Records (EHRs) through a technical framework and standards. The work under eHDSI is funded largely under the EU4Health programme, demonstrating the connection again between the pillars of the model set out in Figure 1. The fact however that the output of the eHealth Network the guidelines to help Member States implement the eHSDI are guidelines, not law, demonstrates also the impact of Article 168 TFEU in ensuring that the power to enact

legislation which defines how health services are provided are still primarily developed at Member State level.

The eHDSI seeks to establish a common framework and technical infrastructure for secure and interoperable sharing of health data across national borders within the EU. Its key objective of the eHDSI is to support safe access to health data to authorised data users for both patient care and healthcare planning and research. It focuses on in particular the use of common technical standards, protocols, and specifications to ensure the seamless exchange and interoperability of health data between different national systems. It also supports compliance with data protection regulations and establishes appropriate governance structures to oversee the secure and lawful sharing of health information. The XpanDH project as a whole is designed to support the up take of tools and measure to address these two core objectives of the eHDSI, while this document seeks to provide an overview of the range of policy and legal instruments that support that wider digital health objective, as well as the specific legal challenges of health data sharing, which are described in Section 5.

4.2 Safe Medicines and Devices

While much of the EU level activity in healthcare is channelled through policy and support, the exceptions to the general principle of subsidiarity provided for in paragraphs (4) and (5) of Article 168 (as described in section 2.1.1. above), allow for very impactful EU level legislation to be adopted which has the general objective of supporting patient safety and the provision of safe medicines and devices on the European Market.

Central to this is the EU level legislation on pharmaceuticals, which are found in the Community code relating to **medicinal products for human use (Directive 2001/83/EC)** and the Community procedures for the authorisation and supervision of medicinal products for human and veterinary use and establishing a European Medicines Agency (Regulation 726/2004) and the legislation on **medicines for children and for rare diseases (Regulation 1901/2006 and Regulation 141/2000** respectively. As medicines have to be developed and trailed as safe for use, the EU has also adopted legislation to ensure that clinical trials are conducted to a common standard across the EU, as set out **in Clinical Trials Regulation (Regulation (EC) 536/2014).** These directives and regulations have been adopted by the European Union on the joint legal bases of Article 168 (4), but as the clinical trials and pharmaceutical legislation does not have a very significant impact on digital health, it will not be detailed further here. It is however a very significant aspect of EU health legislation and impacts every EU citizen every time they take a prescribed or over the counter medication. A small impact on digital aspects of healthcare is foreseen in the proposed revision of Directive 2001/83 which foresees that patient information leaflets should be supported with electronic and digital versions.

Figure 1 also includes two pieces of consumer protection legislation. This is another example of EU law which falls under both the internal market and access to health, having a legal basis in Article 169 TFEU which provides for EU level legislation on consumer protection, which include contributing to "*the health, safety and economic interests of consumers*" (Article 169 TFEU). Two recently adopted pieces of legislation in this area particularly impact digital health: The **Product Safety Regulation (Regulation (EU) 2023/988)** which enters in application on 13 December 2024, and the **Product Liability Directive (Directive 1985/374/EEC)** for which a revision is currently under debate in European Parliament and Council. Both pieces of legislation are generally applicable to medical devices and therefore have application in the area of digital health solutions. This legislation seeks to balance the need to foster safe innovation; provide legal certainty and consistency with the existing legal frameworks and allow consumers to claim compensation if they suffer injury arising from defective products. It should be noted that this general product safety legislation is supported by other legal tools, notable the **Rapid Exchange of Information System** (**RAPEX)** set up by the **Market Surveillance Regulation (Regulation (EU) 2019/1020)**. RAPEX is the Rapid Exchange of Information System which is to alert consumer and suppliers of unsafe consumer products. While RAPEX does not apply pharmaceutical products or medical devices generally, it is important to note that the **proposed European Health Data Space Regulation** states that it will apply to EHR system regulated under that Regulation. Accordingly, a national market surveillance authority will be responsible for ensuring that EHR systems placed on to the EU market are interoperable in the terms of the EHDS Regulation.

The general product safety and liability legislation outlined above l complements the medical device specific legislation found in the **Medical Devices and In Vitro Diagnostic Medical Devices Regulations (MDR/IVDR Regulation 2017/745 and Regulation 2017/746** respectively). The MDR defines medical devices as any instrument, apparatus, appliance, software, material, or other article intended for use in the diagnosis, prevention, monitoring, treatment, or alleviation of disease or injury; although some commentators doubt that the legislation has the capacity to achieve its objectives[9].

Digital health products such as mobile apps, wearable devices, telemedicine platforms, and health software applications are considered medical devices if they have a medical purpose. The MDR provides a framework for the regulation of these devices to ensure their safety, quality, and effectiveness. Under the MDR, digital health products need to comply with the same regulatory requirements as traditional medical devices. This includes conformity assessment procedures, quality management systems, post-market surveillance, and clinical evaluation. The MDR introduces stricter regulations and increased scrutiny for high-risk devices,

[9] Jarman H, Rozenblum S & Huang T (2020). Neither protective nor harmonized: The cross-border regulation of medical devices in the EU. Health Economics, Policy and Law

including those using artificial intelligence or machine learning algorithms. Digital health products also need to be CE-marked, indicating that they comply with the essential requirements of the MDR and have undergone the necessary conformity assessment procedures. The MDR places greater emphasis on the transparency and traceability of devices, including the requirement for a Unique Device Identifier (UDI) to be assigned to each product. Furthermore, the MDR introduces specific provisions for Software as a Medical Device (SaMD). SaMD is defined as software intended to be used for one or more medical purposes without being part of a hardware medical device. The MDR provides guidelines for the classification, clinical evaluation, and post-market surveillance of SaMD. The MDR therefore applies to digital health products that meet the definition of a medical device. These products need to comply with the regulatory requirements of the MDR to ensure their safety and effectiveness in healthcare settings. In the context of XpanDH Member States will want to ensure that all digital health solutions that interface with EHRs are evaluated to establish if they are classified as devices under MDR and is so that they comply with the necessary certification requirements. With respect to the interoperability between digital solutions and EHRs the proposed **European Health Data Space Regulation** discussed below will provide for new certification measures to ensure that such interoperability can be achieved.

4.3 Freedom of movement of goods, workers and services

The internal market is largely defined by freedom of movement. Section 4.1 above shows how free movement of people demands that their social security also moves, and that they can access healthcare, in person or electronically. Healthcare however also demands mobility of workers. Again, COVID demonstrated the need for healthcare professionals and for them to be mobile around the Union. With respect to the right to practice medicine, the **Directive on Mutual Recognition of Professional Qualifications (Directive 2005/36/EC)** applies in principle to all the professions where specific professional qualifications are required to access them under national regulations. The Directive applies to healthcare professionals who want to move physically to provide services in a Member State. However, the Directive applies only where the healthcare practitioner travels to provide the service (either permanently or occasionally); if the service is provided virtually e.g. by remote analysis of an x-ray, then the professional does not need certify the qualifications for the purposes of the Directive, although a service provision contract may still require it. Furthermore, neither **the Directive on Cross Border Care** nor the **Regulation on Social Security** address the possibility of virtual care in which the patient and clinician interact via telehealth technology such as video calling and remote monitoring. Furthermore, neither piece of legislation addresses the situation of a healthcare professional crossing a border to provide care - the focus is patient mobility, not healthcare professional mobility. Wismar et al note in a recent study

that health workforce mobility has been growing with EU enlargements, and has changed directions and magnitude with the economic and financial crisis. The system, the authors note, "while not broken could benefit from some changes to improve the trade-offs between efficiency and equity, between EU labour markets and health systems, between sending and receiving countries and between employers and the health workers. Mobility and cross-border collaboration in the health workforce is essential, especially for smaller countries or in highly specialised ca Although the legislation on professional mobility and cross border care make almost no reference to digital health or the provision of health care through digital means, the EU has adopted significant horizontal legislation on digital services and digital markets recently. The **Digital Services Act (Regulation (EU) 2022/2065)** and **Digital Markets Act (Regulation (EU) 2022/1925)** aim to create a safer digital space where the fundamental rights of users are protected and to establish a level playing field for businesses. Together the two pieces of legislation aim to create a safer digital space in which the fundamental rights of all users of digital services are protected; and to establish a level playing field to foster innovation, growth, and competitiveness, both in the European Single Market and globally. Both pieces of legislation entered into force in late 2022.

The **Digital Services Act** applies to digital intermediary services, such as search engines, digital hosting services and social media platforms. It will therefore apply also to digital health platform services, such as telemedicine platforms, health apps, and online health information portals if they provide information, e.g. links to health services requested by those health service providers. This becomes even clearer if the portal provides recommendation services which suggest or prioritize content, typically products or services to the user. These services would need to comply with certain obligations and requirements, including transparency, user safety, and accountability. The Digital Services Act also addresses the issue of the liability of digital service providers for content shared on their platforms. In the context of healthcare, this could have implications for platforms that host user-generated health information or provide access to health-related content. The law was designed to hold online service providers accountable for their content moderation practices, but also to strike a balance between holding platforms accountable for harmful or illegal content while not imposing excessive burdens that could hinder innovation in the digital health sector.

The **Digital Markets Act (Regulation (EU) 2022/1925)** will similarly have an impact on the healthcare sector in relation to digital platforms and online services that are involved in healthcare services or data exchange. It seeks in particular to address the market power of large online platforms known as "gatekeepers" by imposing specific obligations on them. These obligations include measures to prevent unfair practices, ensure data portability, and promote interoperability and to prevent gatekeepers from engaging in practices that could hinder or limit the access any service provider to their platforms. The objective is to foster a more competitive environment and allow smaller service providers, including healthcare providers or innovative digital

health startups to compete on a level playing field. A key aspect of supporting such a level playing field is to ensure data portability and interoperability. The Digital Markets Act will therefore contribute to the objective pursued by XpanDH insofar as it reinforces the importance of adherence to interoperability standards. However, the Digital Markets Act target 'gatekeepers' who have a significant impact on the EU market, which is defined in Article 3(2) as having a turnover of more than EUR 7.5 billion, or a market value of EUR 75 billion and it has at least 45 million monthly consumer users or 10000 business users. This could include healthcare providers or digital health services. The Digital Markets Act also strengthens certain rights established under the GDPR, including easier data portability. A recent study[10] conducted in Finland noted that patient online social networks and health counselling virtual assistants are also within the scope of the services covered by the DMA. But that it is, however, quite unlikely that digital health service enterprises reach anywhere near the numeric thresholds mentioned in Article 3(2) in their business operation within the EU.

The full impact of these two new pieces of EU level legislation on the health sector remain to be seen, but as digital health grows, it is clear that if a health information system or service is considered being within the scope of the Digital Markets Act or Digital Services Act, scholars such as Varri [10] note that the key issue is to arrange the governance of the system in such a way that the requirements of the act are fulfilled.

5 Data protection

The use of digital solutions in healthcare is defined to a large part by the use of data to provide services to a patient. Access to data plays a crucial role in digital health by enabling the development, implementation, and effectiveness of various healthcare solutions. Access to patient identifiable health data are needed in patient care to provide healthcare professionals with a holistic view of an individual's health status, medical history, and ongoing treatments. This is facilitated by the core tools of digital health: the electronic health record and associate documents, the ePrescription and eDispensation record, as well as electronically shareable laboratory results and medical images. The role of the XpanDH project is to support the implementation of interoperability standards to facilitate access to the data in these core tools in safe manner. Given the centricity of facilitating data use to the mission of XpanDH, this section will take a more didactic approach, to help ensure that project partners are fully aware of the requirements of compliance with data protection legislation. As with other areas of healthcare law discussed in the preceding sections, it is important that project partners use the materials provided

[10] Värri, Alpo Olavi. "The impact of EU Digital Services Act and Digital Markets Act on health information systems." (2023).

here only as a starting point, as national level rules on data protection may have some variation.

Safety in sharing such data may be seen as falling under the so-called triad of **confidentiality, integrity and authenticity**. Confidentiality is largely addressed by **data protection**, with measures designed to prevent sensitive information from unauthorized access. Integrity involves maintaining **data security,** to ensure consistency, accuracy and trustworthiness of data over its entire lifecycle. This is of crucial importance in healthcare to ensure patient safety. It demands that data must not be changed in transit, and steps must be taken to ensure data cannot be altered by unauthorized people for example, in a breach of confidentiality. The role of interoperability standards is of central importance here. However, respect privacy and security must still allow for appropriate **data use** to provide care or for further use in research. This involves properly maintaining hardware and technical infrastructure and systems that hold and display the information.

EU digital health policy addresses all three elements. As noted in Section 4.1 the **eHealth Digital Services Infrastructure** plays a core role supporting safe access to health data, in particular compliance with the legislation that has been adopted at EU level on the legal basis is **Article 16 TFEU** which provides that "*everyone has the right to the protection of personal data concerning them"* and requires the European Parliament and the Council *to lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and rules relating to the free movement of such data"*.

EU level legislation which takes forward the objective of Article 16 TFEU is here discussed under three headings of **data protection**, which is central to the respect of confidentiality; **data security**, which is central to integrity and authenticity; and finally it looks at the challenges of allowing **data use** while still respecting the confidentiality and autonomy of individuals with respect to the way in which data concerning their health are processed both in order to provide care (primary use) and for further secondary use for scientific research and policy making.

5.1 General Data Protection Regulation

The central legislation adopted under Article 16 in force today is the **General Data Protection Regulation (Regulation (EU)2016/679)**, generally known as GDPR. It is considered by many as the world's strongest set of data protection rules, which enhance how people can access information about themselves and places limits on what organizations can do with personal data. The GDPR was enacted in 2016, building on the previous Data Protection Directive of 1995. The new law is a Regulation, not a Directive, meaning that it is directly applicable in every Member State and does not have to be transposed into national legislation. However, despite the fact that the GDPR is a Regulation, it has a number of possibilities for national level variation on key topics, of which use of health data for research purposes is a

key one. The GDPR applies to a wide range of types of personal data, including health related data which recital 35 clarifies includes:

- information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and
- any information on, for example, a disease, disability, disease risk, medical history, clinical treatment, or the physiological or biomedical state of the data subject independent of its source, for example, from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

The key parties which the GDPR addresses are:

- the data subject - in a healthcare setting this includes the patient, but may also include the patient's family who may be involved in care or whose own medical history may be included in notes on a patient. Healthcare professionals will also be data subjects and therefore also have rights under the GDPR
- the data controller and processor - the legal organisation or person who collects and processes data is held accountable for ensuring that the data subject's rights are upheld. This means they have to hold the data securely, processes it according to legal limits and ensure that the data subject can access data concerning them and exercise other rights, including data portability
- the data protection officer and authority – organisations processing large amounts of sensitive data, which will include almost all healthcare providers, are required to appoint a data protection officer who ensures compliance with the GDPR. Each country will also have a data protection authority whose role it is to enforce compliance.

On the matter of co-operation between data protection authorities, in particular in handling complaints that concern more than one EU Member State, a further Regulation to the GDPR[11] was proposed in July 2023 which proposes rules to harmonise and facilitate certain procedural aspects to support more timely and efficient investigations, cooperation and enforcement in complaints procedures involving two or more Member States. The proposed Regulation elaborates in more detail the rights of complainants and the parties under investigation (controllers and processors), with a view to support the smooth functioning of the cooperation and consistency mechanism established by the GDPR.

Huge volumes have been written about GDPR and digital health. The objective here is not to repeat or even provide an overview of all that material, but only to look at the particular challenges of primary and secondary use of data concerning health in

[11] Proposal for a regulation laying down additional procedural rules relating to the enforcement of the General Data Protection Regulation

order through digital health solutions, looking specifically at the duties of data controllers in four categories: **the legal base for data processing; data subjects' rights; and data protection by design.** This does not cover all aspects of GDPR but addresses the most important issues in use of digital health solutions and the remit of XpanDH.

Legal bases for data use

Core to the GDPR is the requirement for lawful data processing and central to the concept of lawfulness is the capacity to comply with one of the legal bases set out in Article 6. In addition, where the data processing concerns sensitive data, such as health related data, the processing of such personal data is in principle prohibited, unless one of the exceptions set out in Article 9(2) applies.

Article 6(1) – Legal bases for processing personal identifiable data

a) **Consent:** the data subject has given consent to the processing of his or her personal data for one or more specific purposes
b) **Contract performance:** processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
c) **Legal obligation:** processing is necessary for compliance with a legal obligation to which the controller is subject
d) Vital interest of individuals: processing is necessary in order to protect the vital interests of the data subject or of another natural person
e) **Public interest**: processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
f) **Legitimate interest**: processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

Figure 2: Legal Bases in GDPR (underlined sections have relevance for healthcare)

Article 9(2) – exceptions to the prohibition on processing sensitive data

a) **Explicit consent**: the data subject has given explicit consent for one or more specific purposes. Consent can also be prohibited by a Member State or EU in specific matters.
b) Employment, social security and social protection: national level legislation may require data processing for carrying out obligations under employment, social security or social protection law, or a collective agreement is allowed if it is authorized by law.
c) Vital interests: where processing is necessary to protect the vital interests of the data subject or of another individual when the data subject is physically or legally unable to give consent.
d) Non-profit bodies: processing under the course of legitimate activities by a foundation, association or another non-profit body with a political, philosophical, religious or trade union aim. The condition is that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes. Also, if the body wants to disclose the data outside the body it needs consent from the data subjects.
e) Data manifestly made public by the data subject: if the data subject themselves makes the sensitive data public, this provides a legitimate reason for further processing the data.
f) Legal claims or judicial acts: processing is valid if it is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
g) **Substantial public interest**: processing is valid under reasons of substantial public interest with a basis in law. Member States can decide the circumstances for the processing of extra sensitive data. The Member States law has to be appropriate to the aim pursued and contain appropriate safeguards measures.
h) **Health or social care with a basis in law**: processing is valid if it is necessary for occupational or preventative medicine or for assessing the working capacity of the employee. The processing must have a base in Member State law or a contract with a health professional. Note that this ground needs obligations of confidentiality between the parties.
i) **Public health with a basis in law**: processing is necessary for reasons of public interest in the area of public health, to protect against serious cross-border threats to health, or to ensure high standards of quality and safety of health care and of medicinal products or medical devices. Note that this ground needs obligations of confidentiality between the parties.
j) **Archiving, research and statistics with a basis in law**: when the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in Article 89(1)

Figure 3: Exceptions of the prohibition in GDPR

Legal bases for use of health data for care provision (primary use)

When data are collected in a healthcare setting such as a doctor's office or a care facility, or in an on-line care setting (such as remote monitoring or support) they are usually collected for the purpose of providing care, because this is the purpose for data collection presented to the patient at the time of data collection. For healthcare professionals the legitimation for processing health data is often found in national level legislation adopted in accordance **Article 6(1)(c) - legal obligation, or Article 6(1)(e) – public interest** and that one of these bases is then coupled **with Article 9(2)(c) legal duty or Article 9(2)(h) - health care or in some cases Article 9(2)(i) - public health** may be used if the purpose is wider public health rather than direct care provision (such as COVID-19 contact tracing). It is possible that Article 9(2)(g)-public interest could also be used, as the duty to collect data may be vested in the

care provider in the exercise of their official duty. It should be noted that all the Article 9(2) exemptions noted above require that EU or national level legislation provides for such data processing. This will usually be found in the national law which regulates healthcare provision and may vary slightly between regions of one country. In addition, it should be noted that a Member State may have further additional legislation on the use of digital health tools which defines which exception should be used. This is seen particularly in countries where a specific digital health law has been adopted, such as the Digital Health Care Act (Digitale-Versorgung-Gesetz) in Germany. A study [12] on the application of the GDPR in the healthcare setting across all Member States published in 2021 found that the most frequently used legal basis and exception for legitimating the processing of health-related data for care provision were Article 6(1)(c) - legal duty used in conjunction with Article 9(2)(h) – healthcare.

An important point to note is that although consent is widely used to legitimate data processing outside the healthcare setting (note for example consent boxes that appear whenever a web site is accessed), consent is rarely used as the legal basis for the processing of health-related information by a healthcare professional. Consent as defined in Article 4(11) GDPR requires that is voluntary and given in the context of a relationship where the data subject has the power to withhold consent without any detriment. This was emphasized in the European Data Protection Board's (EDPB) Guidelines 05/2020 on consent under GDPR, which states that "consent can only be an appropriate lawful basis if a data subject is offered control and is offered a genuine choice with regard to accepting or declining the terms offered or declining them without detriment". It is difficult to meet this requirement in a healthcare setting as it is difficult to provide care to a patient without information about the patient's history, accordingly, sharing such history may not be a free choice if the patient wants to be cared for. Furthermore, the GDPR states that consent may not be appropriate where there is imbalance between the data subject and the controller, in particular where the controller is a public authority. Furthermore, consent can only be used as a legal basis for processing personal data if the data subject can withdraw consent and for such withdrawal of consent to be implemented in a way that all data processing of data concerning that person to stop. This will be very difficult in a healthcare setting where the processing of data is also a record of the act of healthcare. As noted above, many Member States have national level legislation that requires such records to be kept, and indeed further processing may be difficult to exclude if a patient receives any further care, since most national level medical law, as well as good medical practice, requires a healthcare professional to take not to preceding medical history.

[12] Hansen, J., Wilson, P., Verhoeven, E., Kroneman, M., Kirwan, M., Verheij, R., Veen, E.B. van. Assessment of the EU Member States' rules on health data in the light of GDPR. Brussels: Publications Office of the European Union, 2021

Legal bases for use of health data for research (secondary use)

Research is not designated as a lawful purpose in its own right. A legal base in Articles 6 and 9 must therefore be established when secondary use of health-related data. The proposed EHDS is designed to drive a more harmonised approach to the use of the GDPR in this type of data use by providing a legal basis in accordance **with Articles 9(2) (g), (h), (i) and (j) GDPR** for the secondary use of health data. The data user will however still have to demonstrate a legal basis pursuant to Article 6 based on which they could request access to data pursuant to the EHDS Regulation.

Consent for secondary use of health data

It is not yet clear to what extent consent will be used as a legal basis for secondary use of data, as the discussion on the possibility of opting-in or-out of data usage for research by data subjects is still continuing in the European Parliament and Council. While consent to take part in research as a natural person is a key ethical requirement, the legal duty to obtain informed consent about taking part in research lie within the law of medical care, practice and research and is separate from the legal framework for processing data in the context of the research required under the GDPR. As in the case of primary use of data, the GDPR specifically foresees using health-related data without consent for public health purposes. In this context it is important that Recital 54 notes that 'public health' should be interpreted as defined as including "*all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status*."

Data Subjects' rights

The GDPR creates a significant body of data subjects' rights, set out in Articles 12 to 23 of the Regulation, these define an organization's ability to lawfully process personal data.

Right to information

Articles 12-14 set out the data subjects' right to information about what data are collected, how they are to be used, who will have access to them and for how long it will be stored. The requires that the data controller must be named and contact details given (this can be of an organization and role, not necessarily a natural person); and the purpose and legal basis of data processing must be given. This means the legal bases in Article 6(1) and exceptions in Article 9(2) must be explained, this can be done in simple words without reference to the specific articles if this is more appropriate to the target data subject who will be receiving the information about data processing. The data controller will also need to make clear if the data will be shared with any other parties (and a description of such parties), and if the data are to be transferred outside the EU, this must be stated explicitly.

The data controller must also make clear what rights the data subject has (access, rectification etc - see below) and how those rights can be exercised. If the processing is based on consent, the way in which consent can be revoked must be made clear, as well as the right to make a complaint to a supervisory authority. The data subject must also be informed about the existence of automated decision-making, including profiling, referred to in Articles 22(1) and (4) of the Regulation (namely where the profiling produces legal effects or otherwise significantly affects a data subject or involves special categories of personal data). When the controller is engaged in profiling, it also should supply meaningful information about the logic involved, and the significance and envisaged consequences of the processing for the data subject.

Where personal data is collected from the data subject, the information must be provided at the time when the personal data is obtained. When personal data is obtained from someone other than the data subject, the fair processing information should be provided in accordance with Article 14 (3) which states that this must be provided (a) within a reasonable time period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed; (b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or (c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

Given the amount of information which has to be communicated to data subjects under the GDPR, the requirement that what is provided is concise and easy to understand, the challenges posed by new technologies and the potential benefits, in addition to legal compliance, of effective information provision, controllers are likely to benefit from being flexible and creative in their communications with data subjects. The GDPR assists here, as although technology neutral, it recognizes that fair processing information may be most appropriately provided through a number of means depending upon the circumstances of processing (e.g., in writing, through electronic means, orally or using standardized icons).

The right to access, rectification and 'to be forgotten'

The GDPR's right of access set out in Article 15 is in a sense the active counterpart to the more passive right of information in Articles 13 and 14. Any data subject that requests to know must be told about the personal data the organization holds about them and, more specifically, why and how it does so. Most EU Member States have adopted formal Subject Access Request (SAR) processes. Based on having accessed the data held about themselves, the data subject has the right to have any mistake rectified and to have incomplete data completed.

Article 17(1) establishes that data subjects obtain the right to have their personal data erased if any one of the following applies:

- the lawful basis for the processing is the data subject's consent, the data subject withdraws that consent, and no other lawful ground exists;
- the data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing;
- the data has been processed unlawfully;
- erasure is necessary for compliance with EU law or the national law of the relevant member state; or
- the personal data have been collected in relation to the offer of information society services referred to in Article 8(1) of the GDPR.

A key point to note with respect to the right of erasure, is that it will often not apply to health-related data because the data controller does not have to comply with a request for erasure if the data are necessary for the performance of a task carried out in the public interest, such as public health, archiving and scientific, historical research or statistical purposes, insofar as the right to erasure is likely to render impossible or seriously impair the achievement of the objective of research.

Data Portability

Data portability was a new concept introduced by the GDPR, giving data subjects the right to receive their personal data, which they have provided to a controller, in a structured, commonly used and machine-readable format and to transmit the data to another controller without hindrance from the controller. Technically, the controller must either hand the data over to the data subject in a usable fashion, or—at their request (Article 20(2))—transfer the data directly to the recipient of the data subject's choice, where technically feasible. However, the right only arises where data have been collected on the basis of consent or on the basis of a contract, which will not arise frequently in the healthcare setting.

Data Protection by design and by default

The GDPR introduces the idea of data protection by design and by default. This encourages those responsible for design and development to create products with a built-in ability to manage and fulfil and/or which enable data controllers to manage and fulfil all data protection obligations under the Regulation.

Data protection by design aims to ensure that privacy and data protection are integral components of the design and operation of any data processing activities. It requires organisations to consider privacy and data protection measures throughout the entire lifecycle of a system, product, or service that involves the processing of personal data. It involves integrating privacy considerations into the design process, including implementing privacy-enhancing technologies, minimizing data collection and retention, and ensuring transparency in data processing activities. Data Protection by Default requires that the default settings of systems, products, or services should favour privacy and data protection. It means that

individuals should not be required to take additional steps to protect their personal data actively.

Data Protection Impact Assessments

A component of data protection by default is the Data Protection Impact Assessments (DPIAs) to identify and address any data protection issues that may arise any new activities that involve the processing of personal data. The DPIA is considered good practice for all data controllers, but is required when large volumes or sensitive data are processed. Most healthcare organisations will therefore undertake DPIAs when introducing any form of digital health solution. Some Data Protection Authorities list DPIAs as 'best practice' and have issued guidance on how DPIAs should be undertaken.

Under Article 35(7) of the Regulation, the DPIA must contain and document at least the following:

- a systematic description of the envisaged processing operations and the purposes of the processing, including any legitimate interests pursued by the controller;
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of individuals; and
- the measures adopted to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data.

Where, having carried out a DPIA, the DPIA reveals that processing poses a high risk, if there are no measures capable of mitigating the risk, the controller will be required to consult its DPA before commencing processing.

The GDPR is, without doubt, a very important piece of legislation to be considered when new digital health solutions are being implemented. Any organisation procuring or commissioning a digital health solution will need to ensure that the solution is able to meet the requirements of data protection by design, and that the staff and systems of their organisation are able to meet the requirements necessary to provide information to patients and citizens, and to ensure that they are able to exercise their rights.

ePrivacy

The GDPR is complemented by two other generally applicable EU level legislations - the EU Data Protection Regulation, which addresses the way in which the European Institutions can collect and process personal information, and the **ePrivacy Directive (Directive 2002/58/EC)** and proposed **ePrivacy Regulation (Regulation (EU) 2017/101)** which seeks to protect the privacy of EU resident's electronic

communication. As more and more interaction between healthcare professionals and patients occurs via electronic means, this too had an impact on the adoption of digital health solutions.

The ePrivacy Directive was adopted as a complement to the Data Protection Directive to regulate the electronic communication sector specifically. When the European Commission was developing the GDPR it also developed the ePrivacy Regulation, which however still remains a proposal. Its area of application set out in Article 2 is proposed to be *"the processing of electronic communications data carried out in connection with the provision and the use of electronic communications services, and to information related to the terminal equipment of end-users"* when such processing happens on a publicly available network. It includes both electronic communications content and metadata, where 'content' includes text, voice, videos, images, and sound, and 'metadata' refers to data processed to transmit, distribute, or exchange the content.

In a health context this means that when remote patient monitoring happening through a treatment facility's closed network or the patient's home network, the communication will fall outside the definition of "public network". However, once the data leaves this sphere, and is communicated further through a cloud service normally based on a public network where the care unit can access it through an extranet connection. The implant will also have to follow the patient outside the range of their private home networks. It will then connect via typical publicly available cellular communication networks like 4G and 5G. The proposed ePrivacy Regulation is therefore very likely to apply to many digital health solutions and will need to be assessed by the potential users of XpanDH tools just as much as GDPR - not least because both have their legal basis in Article 16 TFEU as well as embracing Article 8 European Charter of Fundamental Rights.

5.2 Data Security

While the law of Data Protection is built very solidly on the foundation of the GDPR, the laws regulating data security are a much more complex weave of legislation that deal cyber security, cyber resilience and network security, with much of this law still in development. However, if the rights enshrined in Article 16 TFEU are to be respected the duties of those responsible for data must include close examination of storage of data in the cloud, and responding to the threat of cyber attacks.

The EU is in the process of adopting a number of new pieces of legislation, and updating other to create a data security package. This include **Network Information Security Directive 2 (Directive 2022/2555/EU)** which was an update to the first NIS directive of 2016 adopted in 2023 which will be applied in the Member States from October 2024. It also includes the **Cyber Security Act (Regulation (EU) 2019/881)** and the ***proposed* Cyber Solidarity Act** and ***proposed* Cyber Resilience Act** In the context of the framework outlined in Figure 1 it is important to note the EU level

legislation in the broad heading of data security are adopted under the internal market competence of the EU (Article 114 TFEU). They are discussed here under the general heading of data protection, because from a healthcare organisation perspective much of the interest in data security is from the perspective of securing data from breach of confidentiality, as well as ensuring that data can be relied upon in terms of integrity and authenticity. However, from a purely European legislative the legislation is adopted in the context of strengthening the internal market.

The Network and Information Security 2 Directive (NIS2)

The NIS Directive has increased the EU national cybersecurity capabilities, requiring Member States to elaborate a National Cybersecurity strategy, establish Computer Security Incident Response Teams (CSIRTs) and appoint NIS national competent authorities. Nevertheless, its implementation proved difficult, resulting in fragmentation at different levels across the internal market. As a response to the growing threats due to digitalization and increase in cyberattacks, NIS2 repeals the existing NIS Directive while broadening its scope, aiming to strengthen the security requirements imposed, addressing security of supply chains, streamlining reporting obligations, introducing more stringent supervisory measures and stricter enforcement requirements including harmonised sanctions regimes across Member States. It also includes proposals for information sharing and cooperation on cyber crisis management at national and EU level.

From the perspective of healthcare provider organisations NIS2 sets important new demands for management bodies of essential and important entities are required to explicitly approve and oversee the implementation of the risk management measures required under the Directive. NIS 2 does not define the term "management bodies", leaving it to the national legislation of individual Member States to define the scope of the term. However, NIS 2's Recital 76 suggests the term refers to senior management and legal representatives. This means that it is highly likely that national level legislation adopted under NIS2 will require the management bodies of health organisations will also have to implement at least the following key measures:

- Risk analysis and information system security policies;
- Incident handling protocols;
- Business continuity plans;
- Supply chain and network security measures;
- Cybersecurity testing;
- Auditing procedures;
- Cybersecurity training
- HR security, access control policies and asset management
- Use of multi-factor authentication and encryption (where appropriate).

By 17 October 2024, the EU Commission will adopt implementing acts which further harmonise and specify the technical and methodological requirements for various entities that often operate cross-border.

Under NIS2, organisations are required to notify any incident (i.e. an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems) that has a significant impact on the provision of their services. The Directive creates the power for national bodies to issues sanctions which include temporary suspension of an authentication or certification to conduct certain activities; orders to implement the recommendations of a security audit; and orders to inform users of a significant cyber threat. Similar to GDPR essential entities (which would include healthcare providers) can be hit with an administrative fine of up to the higher amount of €10 million or 2% of worldwide turnover.

In the context of XpanDH it is therefore crucial to map in more detail the NIS2 requirements that will apply to healthcare organisations who will procure digital health solutions and to develop understanding of the risks core digital health solutions addressed in XpanDH may imply. This would need to be done on a general level, as the Directive will be transposed into national level legislation which may have some variation between Member States.

The Cyber Security Act

The Cyber Security Act (Regulation (EU) 881/2019) provides the baseline for a harmonised European system for the cybersecurity certification of ICT-products, services and processes. The main objective of the Cybersecurity Act (CSA) is to improve protection against threats to cybersecurity within the EU. It has two main functions: to give ENISA (the EU Agency for Network and Information Security) a permanent mandate; and to establish a European cyber security certification framework for ICT (information and communications technology) products, services and processes. The framework sets EU-wide parameters for the rules, technical requirements, standards and procedures surrounding risk-based certification schemes covering different categories of ICT products, processes and services. On 18 April 2023, the Commission ***proposed*** a targeted amendment to the EU **Cybersecurity Act**. The proposed amendment will enable the future adoption of European certification schemes for 'managed security services' covering areas such as incident response, penetration testing, security audits and consultancy. Certification is key to ensure high level of quality and reliability of these highly critical and sensitive cybersecurity services which assist companies and organisations to prevent, detect, respond to or recover from incidents.

From the perspective of digital health, the key element of importance of the Cyber Security Act is the foreseen cloud security certification scheme which is currently a

voluntary certification under the Cybersecurity Act, but is proposed become mandatory for the numerous entities deemed essential or important under the revised NIS2. A technical meeting under the auspices of ENISA's Cybersecurity Certification Conference in May 2023, seeking to gain agreement on the thorny issue of sovereignty, with some types of cloud services being allowed to operate in the EU only if the cloud service is operated by companies based in the EU, with no entity from outside the EU having effective control over the cloud service provider. This requirement is designed to mitigate the risk of non-EU actors undermining EU regulations, norms and values. The current draft certification also requires that all for cloud services would have to be governed by the law of an EU country, and only EU courts, tribunals and arbitration bodies would have jurisdiction for disputes related to the contract. As the new certification process is still in negotiation further detail will be added in the second iteration of this deliverable if it is available at that point in time.

The proposed Cyber Resilience Act and Cyber Solidarity Act

Two further EU level legislative instruments have been proposed by the European Commission. While the NIS2 Directive aims at ensuring a high level of cybersecurity of services provided by essential and important entities, the proposed Cyber Resilience Act (CRA) covers products with digital elements placed on the market. The ***proposed* Cyber Resilience Act** seeks to introduce cybersecurity requirements for all hardware and software products, throughout their whole lifecycle.

The proposed Act has a dual mandate: first, it requires all connected products to be assessed as safe from a cybersecurity viewpoint before being placed on the market, essentially receiving a "compliant" stamp of approval. This stamp of approval can be obtained either demonstrating compliance through self-assessment by the manufacturers (for the majority of hardware and software) or, for "critical products" through third-party assessment. Second, the CRA places a 24-hour time frame obligation for manufacturers to notify competent authorities in case of cybersecurity incidents or active vulnerabilities in the products. Failure to comply with either of these provisions will result in companies incurring in sanctions. "Critical products" are set out in an annex, which includes from products that are used by healthcare providers. Industries from all sectors are affected including routers, VPNs and smart meters, and other digital solutions used in the health sector. The current draft notes in its recitals that EHRs falling under the European Health Data Space Regulation will also fall under the Cyber Resilience Act. This would however be EHRs as products, when the EHR is a Software-as-a-Service offered through a licensing and delivery model, the Cyber Resilience Act would not apply. Similarly, EHR systems that are developed and used in-house are not within the scope of the Act, as they are not placed on the market. It will also not apply to devices that are covered by the MDR or IVDR as compliance with that legislation is seen as sufficient.

The ***proposed*** **Cyber Solidarity Act** aims to strengthen incident detection, situational awareness, and response capabilities, and to ensure that entities providing services critical for day-to-day life can access expert support to manage their cyber risk and respond to incidents. Specifically, it aims to promote information sharing about cyber incidents and vulnerabilities, to help improve the cyber resilience of critical entities, and to create an EU-wide resource for incident management. The Cyber Solidarity Act is a response to the increasing integration of cyber operations in hybrid warfare strategies and the growing number of cyberattacks aimed at cyberespionage, ransomware and disruption. It introduces measures to increase solidarity at Union level for the EU to better detect, prepare for and respond to cybersecurity threats and incidents. The Act is based on three pillars: the deployment of a European Cyber Shield, the creation of a Cyber Emergency Mechanism and the establishment of a Cybersecurity Incident Review Mechanism. The total budget of the Act (including Member States' contribution) is €1.1 billion of which two-thirds will be financed through the Digital Europe Programme. The Act is the last legislative proposal on cybersecurity of the von der Leyen Commission, following the NIS2 Directive and the Cyber Resilience Act.

5.3 Data Use

Digital health needs data - identifiable patient data, and non-personal data from machines and devices, and data measuring footfall, pollution, staff presence and a myriad of other indicators. Such data must be able to flow between the different the professionals in the healthcare systems - doctors, nurses, pharmacists, dentists, administrators, regulators, innovators - and also to patients and their networks as appropriate. As noted at the start of this section, such data use must obey the triad of data values - confidentiality, authenticity and integrity in order that all stakeholders can have trust in its use, but the capacity to access, share and re-use data must also be facilitated.

It is this facilitation of data use that is the focus of the "European Digital Strategy" which has the objective of strengthening mechanisms to increase data availability, to build trust in data exchange and to overcome the technical obstacles to the re-use of data. The latter therefore addresses issues of data interoperability. The **Data Governance Act (Regulation (EU 2002/868)**, which will be applicable after a transitional period from September 2023, is the first of a number of pieces of legislation under the Digital Strategy. However, before discussing the Data Governance Act and the other draft legislation that it has paved the way for, it is important to note that EU level legislation has recently been adopted which addresses electronic identification, which is of course key to sharing patient data in the context of digital health.

Electronic Identification and Trust Service Regulation (eIDAS)

The eIDAS regulation is a European Union Regulation (Regulation 910/2014) was adopted in 2014 to establish a framework for electronic identification and trust services across EU member states. It sets out rules and standards to ensure the legal validity and cross-border recognition of electronic signatures, seals, timestamps, and other electronic trust services.

The regulation promotes the use of electronic identification (eID) to enable individuals and businesses to access online services and conduct transactions securely and conveniently. It establishes a mutual recognition principle, meaning that eIDs issued by one EU member state should be recognized and accepted by other member states.

To ensure the interoperability and cross-border recognition of electronic trust services, eIDAS establishes a framework for the mutual recognition of electronic identification schemes and trust service providers across EU member states. It sets out requirements for the security, integrity, and technical specifications of these services. Overall, the eIDAS regulation aims to create a trusted and secure environment for electronic transactions within the EU. It promotes the use of electronic identification and trust services, ensuring their legal validity and cross-border recognition. The regulation enhances the convenience, efficiency, and reliability of electronic transactions across member states.

A revised version was finalised in June 2021 and is expected to be adopted in late 2023. One of the most significant changes in eIDAS 2 is the broadening of its scope. While the original eIDAS regulation focused primarily on electronic identification, digital signatures, and other trust services, eIDAS 2 expands its reach to encompass new technologies and services. These include mobile identities, digital wallets, and federated identity schemes, among others. This expanded scope ensures that eIDAS 2 remains relevant in today's rapidly changing digital environment, and will impact also digital health solutions, such as ePrescription.The impact of eIDAS2 on XpanDH solutions will be further discussed in the next iteration of this report.

The Data Governance Act (Regulation (EU 2002/868)

The Data Governance Act applies to data held by public sector bodies which is protected on the grounds of commercial confidentiality, statistical confidentiality, protection of intellectual property, and protection of personal data. Thus, personal data held by public sector bodies is covered and hence also the GDPR applies. It does not apply to data held by public undertakings, data held by public service

broadcasters and their subsidiaries, data held by cultural establishments and educational institutions, data protected on the grounds of national security and defence, and data falling outside the scope of the public tasks of the public sector bodies concerned. To ensure that data is properly protected, public sector bodies must ensure that personal data is anonymized and commercially confidential data is properly modified, aggregated or otherwise handled with proper disclosure controls. Thus, the GDPR's concept of pseudonymization is not sufficient: proper anonymization is generally required for reuse of personal data. To help public sector bodies with their new tasks, the Data Governance Act requires Member States to designate specific competent bodies to provide technical guidance for data storage and data processing, help with anonymization, suppression, randomization, and other techniques that ensure privacy, confidentiality, integrity, and accessibility of personal data.

An important new creation of the Data Governance Act is the concept of data intermediation services. This is defined as "a service which aims to establish commercial relationships for the purposes of data sharing between an undetermined number of data subjects and data holders on the one hand and data users on the other, through technical, legal or other means". The work of the data intermediation services will be supervised by competent public authorities that the member states are obliged to designate. The Data Governance Act also creates the concept of data altruism, which is designed to facilitate voluntary sharing of data for wider societal benefits on the basis of data subjects' consent for making data available for general interests including healthcare research. A new element at EU level here is a common consent form for data altruism to be used across all Member States.

From a healthcare perspective the most exciting thing about the Data Governance Act is that it provides the legal basis for the European Health Data Space, which is discussed further below. The Health Data Space is foreseen as one of nine data spaces addressing manufacturing, the green deal, energy, mobility, financial, agriculture, public administration and skills. The health data space is the first one for which a specific law has been proposed. It also paves the way for the Data Act and Artificial Intelligence Act (AI Act) which are listed under the Data Use heading in Figure 1. These three pieces of legislation (EHDS, Data Act and AI Act) will be of major importance to the XpanDH community, however, as they are still in draft and undergoing negotiation in the European Parliament and also in Council, they will be described here only in outline, and then discussed in detail in later interaction of this legislative guide, once final versions have been adopted.

The proposed Data Act

The Data Act, which in July 2023 is in the last rounds of negotiation, creates the framework for sharing and re-use of data generated by using connected products and services related. It includes also data generated by health products, including medical devices and apps. The object is not only to make such data available for

research, but also to give consumers more control over the data generated by the devices and services they use.

The Data Act addresses Business to Consumer (B2C), Business to Business (B2B) and Business to Government (B2G) data sharing. In the B2C and B2B context the Act requires that data is easily accessible by design by in a secure, free of charge and comprehensive format that is commonly used and machine readable. Before the provision of a contract, sellers and renters must provide the information on the type, format and volume of data that the device can generate and the possibilities for the users to the access, delete or retrieve the data. The purposes of data use, potential sharing with third parties and information for the user on how to end sharing of data with third parties must be part of the information provided to the user. The data holder, unless it is a Small and Medium-sized Enterprises (SME), has the obligation to make data available through a simple request. Contractual agreements to restrict or prohibit data sharing are possible only if sharing could undermine a product's security requirements and result in adverse effect on human health, safety or security. In the B2G context authorise the requests from public sector bodies and the Commission, the Central Bank and Union bodies must be to allow them to carry out their statutory duties in the public interest.

The Data Act is subject to the **GDPR**, everything related to the processing of personal data needs to comply with the conditions and rules provided by the GDPR. This means that the Data Act needs to be understood without prejudice to the GDPR, and no provision should be interpreted to diminish the right to privacy. This might however prove difficult as the **Digital Markets Act Regulation** also comes into play, as gatekeepers have been barred from data access rights under the Data Act, which might be incompatible with the GDPR.

The business community has been very concerned that the Data Act could undermine trade secrets and IP security. These fears have been mitigated to some extent by providing a data holder with the right to refuse to share data if there are clearly justified and substantiated reasons for refusing to share data, in particular if serious economic damage to the data holder is highly likely to result from the disclosure of the trade secret or intellectual property.

The proposed European Health Data Space Regulation

The Data Governance Act provides the legal basis for a 'lex specialis' to regulate the sharing of health data. While the proposal, adopted in May 2022 is provided for in the Data Governance Act, its legal base in the TFEU is at the crossroads of the three pillars of law and policy described in this document and in figure 1. The draft law has a dual legal basis in Article 114 TFEU (internal market) and Article 16 TFEU (Data Protection), and will apply without prejudice to the GDPR. The Recitals recall Article 168 TFEU and note that while this means that Member States shall remain

responsible for the organisations of their health services, this should not constitute a barrier to the free movement of digital health services.

The proposed European Health Data Space regulation aims to establish a standardised framework for the collection, storage, use, and sharing of electronic health data both for patient care (primary use) and for re-use of such data for research, policy making and innovation across the healthcare and life sciences spectrum. A key focus is to enhance the interoperability of health data management practices so that data are FAIR – Findable, Accessible, Interoperable, Reusable - both for primary and secondary use. to improve patient care, enhance interoperability, and protect patient privacy.

The regulation emphasises the adoption of interoperable systems that allow seamless exchange of health data among different healthcare providers, ensuring a comprehensive view of a patient's medical history. It encourages the use of standardised data formats, notably the EEHRxF, as well as paving the way for common formats for the other core building blocks of health data, such as electronic, prescriptions and dispensations, laboratory reports and hospital discharge letters.

It aims also to overcome the challenges of varied applications of the GDPR across different EU countries (which that Regulation allows for) by providing a legal basis for data reuse for treatment or research and innovation under GDPR Article 9(2) to ensure that a common approach exists across the the EU. From the XpanDH community perspective the most important elements of this Regulation will be the way in which EHR and other data vehicles' interoperability is to be regulated. It is foreseen that several pieces of secondary legislation - delegated and implementing acts – are to be adopted. The work to be undertaken within XpanDH is intended to support the adoption of such legislation.

The proposed EHDS regulation has generated a huge amount of interest and commentary from healthcare and medical device stakeholders who are core to XpanDH. Most stakeholders appreciate the objectives of improving healthcare outcomes, promoting research and innovation, and facilitating cross-border healthcare cooperation, but there are concerns about data privacy and security of data both from the perspective of data subjects (patients) and in terms of the protection of intellectual property which may be compromised when data from medical devices and clinical trails are made available for secondary use.

Another area of contention is the governance and control of health data. Some stakeholders' express concerns about the potential concentration of data in the hands of a few entities, such as big tech companies or governmental bodies. They emphasise the importance of ensuring equitable access to health data for all stakeholders, including healthcare providers, researchers, and innovative startups. There are calls for a balanced approach that protects patient privacy while fostering innovation and competition.

The emphasis on interoperability of health data systems is generally welcomed, but there is concern that its demands could create costs for both data holders (especially device manufacturers) and also for the Member States as they build the systems the new legislation calls for.

Furthermore, stakeholders emphasize the need for strong data governance frameworks and mechanisms for accountability and transparency. They call for involvement from all relevant stakeholders, including patients, healthcare professionals, researchers, and industry representatives, in shaping the policies and governance structures of the European Health Data Space.

These issues will be discussed in detail in the next iteration, when the text of the draft legislation is finalised.

The proposed Artificial Intelligence Act

The proposed EU Artificial Intelligence Act aims to regulate the development, deployment, and use of artificial intelligence (AI) systems within the European Union. It seeks to ensure that AI technologies are developed and used in a manner that is trustworthy, transparent, and aligned with fundamental rights and values.

The Act classifies AI systems into four categories: unacceptable risk, high risk, limited risk, and minimal risk. Unacceptable risk AI systems, such as those used for social scoring or biometric identification, would be banned. High-risk AI systems, like those used in critical infrastructure, law enforcement, or healthcare, would require strict conformity assessments and meet specific requirements regarding transparency, accuracy, and human oversight. They also include all medical devices which require third party classification under the MDR – see further below.

The Act emphasises the need for transparency and accountability in AI systems. It requires providers to provide detailed documentation and information about the AI's capabilities, limitations, and potential biases. Users must also be informed when they are interacting with an AI system and be made aware of its limitations. To ensure compliance, the Act proposes the establishment of a European Artificial Intelligence Board and a network of national AI regulatory authorities. These bodies will be responsible for issuing guidance, supervising compliance, and enforcing the regulations.

Additionally, the Act addresses issues related to data and data access. It emphasises that AI systems should be trained on high-quality, unbiased data and that datasets used for AI development should not perpetuate discrimination or biases. It also encourages data sharing and access, particularly for public interest purposes. Overall, the proposed EU Artificial Intelligence Act aims to create a harmonised regulatory framework for AI systems in the European Union. By promoting transparency, accountability, and adherence to fundamental rights, the Act seeks to foster trust in AI technologies and ensure their responsible development and use within the EU.

The proposed EU Artificial Intelligence Act has generated mixed reactions from healthcare and medical device stakeholders. Some have expressed support for the Act's focus on ensuring the safety and transparency of AI systems used in healthcare. They believe that the Act's regulations can enhance patient safety, improve diagnostic accuracy, and enable more efficient healthcare delivery. However, there are concerns about the Act's potential impact on innovation and the development of AI technologies in healthcare. Critics argue that the Act's stringent regulatory requirements, particularly for high-risk AI systems, may hinder the adoption of innovative AI solutions. They fear that the lengthy conformity assessment processes and strict oversight could slow down the development and deployment of AI applications in healthcare. Another concern is the Act's definition of high-risk AI systems, which some stakeholders find overly broad. They worry that this broad definition might encompass a wide range of AI applications, potentially subjecting many healthcare and medical device companies to burdensome regulatory requirements, even if their AI systems pose minimal risks. Generally, in order to address the practical implementation and enforcement of the Act, the need for clear guidelines and consistent interpretation of the regulations to ensure effective compliance has been emphasised.

Generally, while there is support for the Act's intentions to enhance patient safety and transparency in AI systems used in healthcare, concerns remain about potential negative impacts on innovation, the broad definition of high-risk AI systems, practical implementation, and coordination with existing regulations. As for the EHDS Regulation, the next iteration of this report will provide detailed commentary on its potential impact on the use of digital health technologies.

6. End Note

In this document we have provided an overview of a wide range of legislation that impact the adoption of digital health solutions in the Member States. It seeks to demonstrate the breadth of the legislation and its integration, focusing on the balance between the support and growth of the internal market based on data on the one hand, and the respect for privacy and data protection on the other; and placing this in the overall context of the European Union's commitment to the health of its citizens, while at the same time respecting the right of Member States to organise their healthcare systems.

As noted, this is a first iteration. This will in the second iteration become the background chapter of a document whichever looks more closely at the health sector specific legislation which is currently still in negotiation. It will look in particular at the implementation of the EHDS Regulation and its interaction with, and legal interoperability with the Medical Devices Regulation and other relevant legislation. It will focus in particular on new legislation on data security and its role in driving trust in digital health solutions.