

ARTICLE

Data Sharing in the Internet of Medical Things: Between the Data Act and the EHDS

F. Casarosa  and F. Gennari 

Liderlab – Dirpolis, Sant’Anna School of Advanced Studies, Pisa, Italy

Corresponding author: F. Casarosa; Email: federica.casarosa@santannapisa.it

Summary

Healthcare systems are increasingly exploiting the advantages of Internet of Things technologies: cloud-connected devices with perceptive sensors can gather very accurate health data from people even if they do not get to the hospital or private clinics. For potential innovators of new medical IoT devices, the legal framework applicable was until now limited to the application of the General Data Protection Regulation and the Medical Devices Regulation.

This paper will investigate what will happen when medical IoT-generated data are shared to create new products or services according to the framework now depicted by the Data Act and the European Health Data Space.

Given that the EHDS and the Data Act are both aimed at facilitating the secondary use of (health) data, the contribution will compare the two processes set up to establish a roadmap to solve health-data sharing theoretical and practical queries.

Keywords: connected products; data access; data sharing contracts; data transfer; Internet of Medical Things; secondary use of health data

I. Introduction

Internet of Things (IoT) is the terminology used to describe an ecosystem of objects and devices which can gather information on the surrounding environment with sensors. This type of technology can be applied in many sectors as it can adapt to different tools and applications. The easiest example is the case of smart objects installed in a smart house: from the smart fridge to the smart lighting, the devices are all connected to the internet and can gather information from the user and react to specific requests.¹ Still, the sector where IoT use is flourishing is the health one: wearable or implantable devices gather information about patient’s health conditions, allow doctors (or hospitals) to personalise medical services, and react expeditiously to emergencies.² During the Covid pandemic, the use of such technologies was crucial to avoid direct contact between patients and doctors without reducing the possibility of providing

¹ L Vizzoni, *Domotica e diritto. Problemi giuridici della smart home tra tutele e responsabilità* (Giuffrè Milano 2021); J Chen and Others, “Who Is Responsible for Data Processing in Smart Homes? Reconsidering Joint Controllership and the Household Exemption” (2020) 10 *International Data Privacy Law* 279.

² J Chanachujit and Others, *Healthcare 4.0: Next Generation Processes with the Latest Technologies* (Springer Singapore 2019) 24 available at <<http://link.springer.com/10.1007/978-981-13-8114-0>> (last accessed 25 August 2023); A Chacko and T Hayajneh, “Security and Privacy Issues with IoT in Healthcare” (2018) 4 *EAI Endorsed Transactions on Pervasive Health and Technology* 1.

medical care.³ Moreover, IoTs in the health sector are also perceived as tools to increase the system's efficiency: the cost of unnecessary check-ups is reduced, as the patient is constantly monitored.

The Covid pandemic has also confirmed the value of health data for research activities: thanks to the clinical and immunological data gathered from patients who were already affected and survived the disease, it was possible to understand the virus and its structure and to predict which of its components will provoke an immune response.⁴ This was a key step in vaccine design and allowed research teams worldwide to build up the necessary knowledge to eventually produce an effective vaccine.

As a matter of fact, the data gathered by IoT devices can subsequently be used for research activities, both to improve the device itself and to develop new tools or devices. This type of processing is crucial for innovation in the health sector, as it allows researchers and manufacturers to verify the potential avenues for improvements and to test and train new products on real and reliable data. However, when the data needed in this subsequent development are personal data, some limitations apply. In particular, the General Data Protection Regulation allows the "secondary" use of personal data only for specific circumstances, such as for research purposes or public interest in public health.⁵ Yet, two recent European legislations were put forward to enhance the opportunities for the secondary use of personal data: the Data Act (DA) and the European Health Data Space Regulation (EHDS). Although the two legislative acts rely on the framework provided by the General Data Protection Regulation, inconsistencies and lack of coordination among the three legislative interventions emerge. In particular, interrelated issues emerge across the set of legislations, such as incoherent terminology used, the overall complexity of the application, as well as intra-related issues affecting the economic incentives for market actors to exploit the path provided by each piece of legislation. Moreover, the use of IoT in the health sector may imply the application of another piece of legislation: the Medical Device Regulation, depending on the type of purposes of the IoT devices considered.

This contribution will address the overlaps and the coordination issues applicable in the case of medical IoT investigating what will happen when IoT-generated data are shared to create new products or services according to the framework now depicted by the Data Act and the European Health Data Space. Given that the EHDS and the Data Act are both aimed at facilitating the secondary use of (health) data, the contribution will compare the two processes set up to establish a roadmap to solve health-data sharing theoretical and practical queries.

The article will first identify the current legislation applicable to IoT in the medical sector, looking to the General Data Protection Regulation and the Medical Device Regulation. Then, the specific case of secondary use of data will be presented, comparing the rules in the DA (Section 3) and the ones in the EHDS (Section 4). An evaluation of the most suitable solutions from the manufacturer's perspective will be presented in the conclusions.

³ M Kamal, A Aljohani and E Alanazi, "IoT Meets COVID-19: Status, Challenges, and Opportunities" (arXiv, 28 June 2020) available at <<http://arxiv.org/abs/2007.12268>> (last accessed 25 August 2023).

⁴ H Dögg Gunnarsdóttir and Others, "The Ethics and Laws of Medical Big Data" in M Ienca and Others (eds), *The Cambridge Handbook of Information Technology, Life Sciences and Human Rights* (1st edn, Cambridge University Press 2022) available at <https://www.cambridge.org/core/product/identifier/9781108775038%23CN-bp-4/type/book_part> (last accessed 25 August 2023).

⁵ J Vukovic and Others, "Enablers and Barriers to the Secondary Use of Health Data in Europe: General Data Protection Regulation Perspective" (2022) 80 Archives of Public Health 115; R Becker and Others, "Applying GDPR Roles and Responsibilities to Scientific Data Sharing" (2022) 12 International Data Privacy Law 207.

II. The data processing in Medical IOT

I The general data protection regulation framework

The personal data collection carried out by any connected product or IoT is subject to the rules provided by the General Data Protection Regulation (GDPR), which identifies a horizontal framework applicable to data processing with special attention to health data.⁶

The GDPR applies to any operation or set of operations performed manually or by automated means on personal data (Article 4 (2) GDPR). According to the definition provided by GDPR, personal data includes any information related to an identified or identifiable natural person. Thus, personal data can be objective information, such as the features of the individual, which rarely change (eg, the colour of the eyes or the place of birth), and subjective information, such as opinions or assessments. The GDPR does not distinguish between objective and subjective data but rather between generic data and special categories of personal data. The second category includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data, data concerning health, etc. (Article 9 GDPR). In this latter case, stricter rules apply to data processing. Although Article 4(15) GDR provides a definition of health data, the terminology used is not clear, as health data are “personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.” This almost tautological definition⁷ may lead to an extremely wide interpretation that can also cover other personal data that indirectly hint at the health conditions of the data subject.⁸

IoT processing of personal data that concerns health is therefore subject to the stricter requirements imposed by Article 9 GDPR.⁹ Health data processing is prohibited except for a set of specific legal cases, such as upon the special consent by the data subject, data manifestly made public by the data subject, data processing aimed at preventive or occupational medicine and also data processing for reasons of public interest in the area of public health.¹⁰ These exceptions are crucial for the secondary use of health data, as will be clarified in the section dedicated to the EHDS.

Looking in general at the actors involved in the data collection carried out by a connected product, we may distinguish between three types of actors that can collect and process the personal data of the data subject, namely the data controller, the data processor and the data recipient.

Article 4(7) GDPR describes the data controller as “the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.” Given the crucial role played by

⁶ The literature focusing on the GDPR is extremely wide, the most comprehensive analysis can be found in L Feiler, *The EU General Data Protection Regulation (GDPR): A Commentary* (Globe Law and Business Working 2018); I Spiecker genannt Döhmann and Others, *General Data Protection Regulation: Article-by-Article Commentary* (First edition, Beck Munchen 2023); P Voigt, *The EU General Data Protection Regulation (GDPR) A Practical Guide* (1st ed. 2017., Springer International Publishing Cham 2017); I Kamara, E Kosta and R Leenes (eds), “Research Handbook on EU Data Protection Law” in *Research Handbook on EU Data Protection Law* (Edward Elgar Publishing Cham 2022) available at <<https://www.elgaronline.com/edcollbook/edcoll/9781800371675/9781800371675.xml>> (last accessed 25 June 2024).

⁷ M Tzanou (ed), *Health Data Privacy under the GDPR: Big Data Challenges and Regulatory Responses* (Routledge New York 2021) 6.

⁸ For a risk-based approach to the definition of health data, see W Schäfke-Zell, “Revisiting the Definition of Health Data in the Age of Digitalized Health Care” (2022) 12 *International Data Privacy Law* 33.

⁹ See health data definition in Art 4(15) GDPR. Note that academic literature has highlighted the lack of clarity in this definition see Tzanou (n 7); T Mulder, “The Protection of Data Concerning Health in Europe” (2019) 5 *European Data Protection Law Review* 209.

¹⁰ See that Art 9 (2) lists ten categories of exemptions.

the data controller in the processing, the GDPR adopts an objective approach to identifying who oversees this role, looking at the factual elements or circumstances of a case, regardless of any formal declaration.¹¹ The controller is the body that decides the purpose of the processing and means to carry it out: the type of data collected, the duration of the process, the recipients of data, and the technical means to process the data. It should be underlined that the data controller is not obliged to control the means physically or directly; it is possible that the hardware or software collecting personal data is entrusted to a third party. This is relevant in the case of IoT in the medical sector; for instance, the company manufacturing the software that is embedded in a device that monitors blood sugar levels for patient subjects with diabetes can be qualified as a data controller as it processes the health data to provide an alert if the level of sugar in the blood rises. Still, data collection can be done thanks to sensors collecting raw data from the data subject's body; such sensors can be part of a multi-purpose (smart) device that runs more than one software.

The data processor, pursuant to Article 4(8) GDPR is the natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. The processors involved in data processing may be more than one and oversee different processing stages. Also, in this case, the factual circumstances and the concrete activities are crucial to identify whether the qualification as a data processor is correct. For instance, the provided service may not be targeted at processing personal data or does not constitute a key element of the service. In these cases, the service provider cannot qualify as a processor but as a data controller. A different situation may emerge when the data processor decides to carry out additional processing for its own purpose with the data collected; in this case, the qualification is correct as the data processor was under the direct control or authority of the data controller, but the additional processing may lead to an infringement of Article 28(10) GDPR.

The role of the data controller and the data processor can be clearly identified in the processor agreement, where the services offered by the data processor are presented, and the final approval of the data controller allows for their adoption in the data processing. For instance, in case the IoT is a smart device with limited internal memory, it may use the services of a cloud storage provider. Although the cloud service can be completely standardised, with limited to no power to change the contractual clauses, the IoT developer will play the role of the controller, given its decision to use this particular cloud service provider to process personal data for its purposes. In contrast, the cloud service provider will qualify as a data processor.¹²

Article 4(9) GDPR adds another actor who may play an important role in the data processing, namely the data recipient, who is defined as “a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.” In principle, the data recipient has no obligations or responsibilities vis-à-vis the existing data processing. However, it can become a new controller or processor once the data are received. For example, when a controller sends personal data to another entity, the latter is qualified as a recipient. This disclosure may be justified for

¹¹ EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 7 July 2021, available at <https://www.edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf>, p. 13.

¹² Note that the EDPB clarify that the presence (or absence) of a written arrangement, however, is not decisive for the existence of a controller-processor relationship, as also, in the absence of a written processing agreement, the relationship may emerge from the factual circumstances of the case. However, the absence of a clear definition of the relationship between the controller and the processor may raise the problem of the lack of a legal basis on which every processing should be based, eg, with respect to the communication of data between the controller and the alleged processor. See EDPB (n 11), 32.

data sharing, transmission or dissemination. For instance, the IoT manufacturer may disclose the data processed to parent companies for advertising purposes.

2. The specific rules emerging from the Medical Device Regulation

Another regulation that may apply to the IoT in the health sector is the Medical Devices Regulation 2017/745 (MDR).¹³ The MDR replaced two previous medical device directives (Council Directive 90/385/EEC on Active Implantable Medical Devices (the AIMD) and Council Directive 93/42/EEC on Medical Devices (the MDD) on 26 May 2021).¹⁴ The new legal framework also brought some novelties regarding the definition of medical devices.¹⁵

IoT devices can be qualified as medical devices. According to Art. 2(1) MDR, a medical device is “any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings” for one of the specific objectives listed in the subsequent lines of the same article.¹⁶ The important update is the inclusion of “software” among the types of medical devices, both stand-alone software and software connected to other software, and also software offered as a service to another medical device.¹⁷ It is important to note that when the software qualifies as an accessory, ie, it can steer the performance of a device, but as a stand-alone component does not perform medical actions, it does not qualify as a medical device.¹⁸ However, the definition of medical device (MD) software is ambiguous: if MD software is downloaded on an IoT, does this new connected product with a related service constitute a new IoMT? In the least problematic scenario, the reply is negative: the IoT object can be considered an accessory to the MD software.¹⁹ However, it is possible that the IoT is already a medical device whose functioning is enhanced by MD software. Thus, the

¹³ The MDR Regulation is linked to Regulation 2017/746 on in vitro diagnostic medical devices, and it repeals Directive 98/79/EC and Commission Decision 2010/227/EU. However, the latter is beyond the scope of this analysis.

¹⁴ Note that the revision of the legislative framework was triggered by the so-called PIP scandal, which threatened the safety of more than 400 thousand women using industrial silicone in breast implants.

¹⁵ T Mulder, “The impact of the European Medical Device Regulations on the development and use of mHealth apps in Europe” in J Madir (ed), *HealthTech* (Edward Elgar Publishing Cham 2020) available at <https://www.elgaronline.com/view/edcoll/9781839104893/24_chapter13.xhtml> (last accessed 25 August 2023); H Yu, “Regulation of Digital Health Technologies in the European Union: Intended versus Actual Use*” in I Glenn Cohen and Others (eds), *The Future of Medical Device Regulation* (1st edn, Cambridge University Press 2022) 103 available at <https://www.cambridge.org/core/product/identifier/9781108975452%23CN-bp-8/type/book_part> (last accessed 25 August 2023); K Biczysko-Pudelko, “The Regulatory Environment for the Safety of the Internet of Medical Devices Users in the European Union and the United States” (2024) 15 *European Journal of Risk Regulation* 887.

¹⁶ The list is as follows: diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease; diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability; investigation, replacement or modification of the anatomy or of a physiological or pathological process or state; and providing information by means of *in vitro* examination of specimens derived from the human body, including organ, blood and tissue donations, and which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such means.

¹⁷ “Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 –MDR and Regulation (EU) 2017/746- IVDR” (MDCG 2019) 11; K Ludvigsen, S Nagaraja and A Daly, “When Is Software a Medical Device? Understanding and Determining the ‘Intention’ and Requirements for Software as a Medical Device in European Union Law” (2022) 13 *European Journal of Risk Regulation* 78.

¹⁸ See Recital 12 MDR.

¹⁹ Art 2 (2) MDR.

reply to the previous question can be positive: it is a new medical device, a generic device group²⁰ or a system.²¹

Moreover, the definition in Article 2 (1) MDR provides the criteria distinguishing medical and wellness devices/software.²² If the purpose is among the ones listed, the device/software qualifies as a medical device. Article 2 (12) MDR states that the purpose is indicated by the manufacturer. Therefore, it is up to the manufacturer to provide information about the device's purpose on the label, in the instructions for use or in promotional or sales materials or statements.

The MDR refers to the GDPR in terms of protecting personal data, according to Article 110 MDR. Thus, the roles of the data controller and/or processor can be found in the data processing carried out by the medical device. As a result of the previous description, it is possible to identify and distinguish different hypotheses depending on the technical features of the IoMT. The most common one is the case of an IoMT as a standalone device: here, the role of the data controller can be allocated to the device's manufacturer. However, depending on the possibility for a medical expert to verify the results of the device applied to a patient, a joint controllership with the medical expert may occur. This is the case with HomeKit Lite,²³ which is a standalone certified medical device designed for the rehabilitation of cognitive patients both at the hospital and at home. The device includes a set of components and sensors that allow the patient to perform several exercises: cognitive exercises, but also speech therapy, postural, facial, respiratory, motor and neuromotor skills exercises. The system can be used offline, collecting information about the activities of the patient and in connection with the therapist, who can monitor the previous results collected by the device and adapt to the needs of the patient. In this case, although the medical device is a standalone device that does not exploit any external service for storage and processing (such as cloud computing service), health data regarding the patient are also shared directly with the therapist.

So far, the legislation applicable to data processing by medical IoT has been limited to the aforementioned provisions of the GDPR and MDR. Suppose manufacturers are interested in developing novel IoT in the medical sector, such as applications and devices that complement existing devices. In that case, they cannot exploit the data structures already available in the existing devices. For instance, developing an AI-based medical software that allows the recognition of tumoral formations may be better trained and tested with the data and patterns detected by existing medical devices. In this case, the manufacturer may be unable to access such data, except for applying the specific exceptions provided in Articles 6 and 9 GDPR.²⁴ Moreover, the conditions upon which the data are shared are not defined in GDPR, and, for instance, where specific interoperability

²⁰ Art 2(7) MDR. It refers to '[...] set of devices having the same or similar intended purposes or a commonality of technology allowing them to be classified in a generic manner not reflecting specific characteristics'.

²¹ Art 2(11) MDR. According to the Art. a system "means a combination of products, either packaged together or not, which are intended to be inter-connected or combined to achieve a specific medical purpose".

²² H Van Kolschooten, "The mHealth Power Paradox: Improving Data Protection in Health Apps through Self-Regulation in the European Union" in I Glenn Cohen and Others (eds), *The Future of Medical Device Regulation* (1st edn, Cambridge University Press 2022) available at <https://www.cambridge.org/core/product/identifier/9781108975452%23CN-bp-5/type/book_part> (last accessed 25 August 2023).

²³ See at available at <<https://khymeia.com/en/products/homekit/>>.

²⁴ R Becker and Others, "Secondary Use of Personal Health Data: When Is It 'Further Processing' Under the GDPR, and What Are the Implications for Data Controllers?" (2022) 30 *European Journal of Health Law* 129; S Slokenberga, "Scientific Research Regime 2.0? Transformations of the Research Regime and the Protection of the Data Subject That the Proposed EHDS Regulation Promises to Bring Along" (2022) 2022 *Technology and Regulation* 135; M Shabani and S Yilmaz, "Lawfulness in Secondary Use of Health Data Interplay between Three Regulatory Frameworks of GDPR, DGA & EHDS" (2022) 2022 *Technology and Regulation* 128. Note that in some cases, pursuant Art 9 (4) GDPR, Member States retain the freedom to envisage higher level of protection or the possibility to set limitation to processing of health and genetic data.

standards are relevant for the interpretation and use of the data, the lack of coordination and coherence may reduce the advantages of the data sharing. These limitations are addressed and tentatively solved by the Data Act and the EHDS legislation recently adopted.

III. The impact of the data act on the development of new medical IoT

Medical IoT fall into the scope application of the Data Act (DA).²⁵ To clarify how the DA will affect the choices of manufacturers, it is necessary to understand the rationale of this piece of legislation by comparing it with the structure and functioning of a medical IoT (3.1). Second, the DA's functioning will be described, focusing on the data-sharing contract schemes and their applicability to IoMT (3.2). Finally, overlaps, clashes, and possible harmonisation of the DA data sharing involved subjects with the GDPR ones will be addressed (3.3).²⁶

I. The origin and the rationales of the DA and why it applies to the IoMT

The DA must be considered when discussing IoMT objects' data-sharing practices for two reasons. First, it is the most general (ie, horizontal) regulation concerning data sharing and concerns both personal (health) data and non-personal data, as stated by Art. 1(1) and (2) DA. The DA aims to build up on the GDPR and Free Flow of Data Initiative²⁷ data sharing principles and to apply them to data-reliant new technologies such as the IoT but also, in perspective, some kinds of AI. In the absence of a sectorial intervention, the DA will be applicable to business-to-business (B2B) – more likely – and business-to-consumer (B2C) – less likely – health data-sharing scenarios among a set of subjects. It is also noteworthy to point out that this data-sharing will be regulated through contractual agreements.²⁸ Second, one of the objectives of the DA is to make available “[...] product data and related service data to the user of the connected product or related service” (Art. 1(a) DA). Product data is generated by a connected product, which is none other than an IoT object.²⁹ In fact, Article 2(5) DA

²⁵ Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) PE/49/2023/REV/ OJ L, 2023/2854, available at <<http://data.europa.eu/eli/reg/2023/2854/oj>> (last accessed 22 December 2023). In this part of the article, there will be frequent comparisons with the previous Data Act proposal (DA proposal) whose bibliographic references are the following: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act) COM/2022/68 final.

²⁶ As a methodological limitation, we will not consider the cybersecurity perspective. In this case, as far as IoMT is concerned, the MDR provides manufacturers with cybersecurity duties for medical devices.

²⁷ Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance.)

PE/53/2018/REV/1 OJ L 303, 28.11.2018, p. 59–68, available at <<http://data.europa.eu/eli/reg/2018/1807/oj>>.

²⁸ LA Bygrave, “The Predilection for Contract in Governing Digital Networks: Micro-Management’s Face Off with Accountability” (2023) available at <<https://papers.ssrn.com/abstract=4417972>> (last accessed 18 January 2024); L Trakman, R Walters and B Zeller, “Is Privacy and Personal Data Set to Become the New Intellectual Property?” (3 September 2019) available at <<https://papers.ssrn.com/abstract=3448959>> (last accessed 17 January 2024); H Ullrich, “Technology Protection and Competition Policy for the Information Economy. From Property Rights for Competition to Competition Without Proper Rights?” (14 January 2020) available at <<https://papers.ssrn.com/abstract=3437177>> (last accessed 17 January 2024); Drexl and Josef, “Designing Competitive Markets for Data (2017) 8 Designing Competitive Markets for Industrial Data Between Propertisation and Access 257.”

²⁹ D Bandyopadhyay and J Sen, “Internet of Things: Applications and Challenges in Technology and Standardization” (2011) 58 *Wireless Personal Communications* 49; A Rayes and S Salam, *Internet of Things From*

describes the “connected product as ‘[...] an item that obtains, generates or collects data concerning its use or environment and that is able to communicate the product data via an electronic communications service, physical connection or on-device access, and whose primary function is not the storing, processing or transmission of data on behalf of any party other than the user.’”³⁰ The DA definition is more detailed concerning how the IoMT works while connected to other IoTs, sockets or the human body and the choices for it to be accessed. Because of the generality of this definition, an IoMT as well, such as a wearable heart monitor device, is a kind of connected product.

Regarding the technologies considered, the DA considers the AI, especially when it deals with related service data, which are generated by “related services.” The definition considers three aspects: first, the service is integrated in some way into the product (eg, by being downloaded); and second, “its absence would prevent the connected product from performing one or more of its functions”; and third, “which is subsequently connected to the product by the manufacturer or a third party to add to, update or adapt the functions of the connected product.”³¹

2. The DA framework

To explain the DA’s application, it is necessary first to describe the subjects involved in the data sharing and, secondly, to analyse the structure of the future data-sharing contracts based on the DA itself.

(a) *Who is who? The data-sharing subjects*

The subjects involved in the data-sharing contracts are mainly three.

The first is the **user**, who can be a consumer or a professional. Article 2(12) DA states that the user is either a natural or legal person “that owns a connected product or to whom temporary rights to use that connected product have been contractually transferred, or that receives related services.”³² However, in the framework of IoMT, it is unlikely that the patient/consumer using an IoMT or MD software has the knowledge, resources and initiative to enter into a data-sharing contract. It will be more likely that the data-sharing contract will be negotiated by a professional, such as a doctor, or a health facility that purchased or rents an IoMT object (such as a smart IoMT for a distance heart monitoring

Hype to Reality: The Road to Digitization (Springer International Publishing 2019) available at <<http://link.springer.com/10.1007/978-3-319-99516-8>> (last accessed 16 October 2023).

³⁰ This definition is more detailed compared to the initial proposal’s definition of (just) product, which reads in the following way “‘product’ means a tangible, movable item, including where incorporated in an immovable item, that obtains, generates or collects, data concerning its use or environment, and that is able to communicate data via a publicly available electronic communications service and whose primary function is not the storing and processing of data.’”

³¹ Art 2(6) DA.

³² It is important to note that Art 20 GDPR already envisaged the possibility for the data subject to exercise their right to data portability, allowing also the possibility to transfer the data from one controller to another. However, some differences emerge from the Data Act framework. First, according to Art 20 GDPR, the right can be exercised regardless of the justification to ask for the data, while the Data Act envisages a specific innovation purpose which requires additional guarantees for the data controller. Moreover, Art 20 GDPR focuses on personal data provided by the data subject to a data controller, while the Data Act acknowledges the possibility of sharing “product data and related service data, including the relevant metadata necessary to interpret and use those data” (Art 3 DA). Therefore, the type of data shared is wider. Additionally, it must be stressed that the practical application of Art 20 GDPR was still limited, and the Data Act may be interpreted as a way to make the right to data portability actionable. See available at <<https://mydata.org/2022/02/25/eu-data-act-making-data-portability-actionable/>>.

object) or related service-MD software (such as an AI-based image diagnostic application for tumours).

The second is the **data holder**. Article 2(13) DA describes it as “a natural or legal person that has the right or obligation [...] to use and make available data, including, where contractually agreed, product data or related service data which it has retrieved or generated during the provision of a related service.” Following the previous examples, the data holder could be the manufacturer of the connected product, meaning the company marketing the distance health monitoring IoMT, or the developer of the related service developed, such as the AI-based image diagnostic application for tumours.

The last subject is the **data recipient**. According to Article 2(14) DA the data recipient is “a natural or legal person, acting for purposes which are related to that person’s trade, business, craft or profession, other than the user of a connected product or related service, to whom the data holder makes data available, including a third party following a request by the user to the data holder or in accordance with a legal obligation under Union law or national legislation adopted in accordance with Union law.” Thus, the data recipient differs from the user and must act for professional (*lato sensu*) reasons. Besides, the data recipient cannot be a data holder, as it is specified that it must receive data from the data holder itself. It can be, though a **third party** who received authorisation from the user to ask for access to data to the data holder. This data recipient/third party can also act autonomously, but only if there is a legal obligation under EU or national law implementing the EU law. This last possibility seems to fit with the hypothesis of mandatory data sharing with EU institutions and bodies whenever an emergency arises.³³ Keeping the previous examples, the third party can be an MD or a software company that wants to develop new software applications that can be compatible with the heart-monitoring IoMT, such as e-wellness apps. As far as the second example, a medical devices company developing IoMT, such as radio or chemotherapy medical devices, might be interested in having access to the AI-based diagnostic program data to understand which kind of tumour is more frequent and how it is distributed among a target population, such as the hospital patients for which this software has been used for diagnostic purposes.

(b) *The data-sharing contract schemes*

Two kinds of data-sharing contracts are set in Articles 4 and 5 of the DA. The first one is characterised by the absence of any intermediary between the user and the data holder; the second one, instead, is multifaceted, as it requires a triangulation of contracts involving the user, the data holder and the data recipient/third party.

(i) *The user and data holder. A relationship without intermediaries.* In this scenario, there are two parties: the user and the data holder. The user who wants to access the connected product or related service data to develop another connected product or related service. This new connected product or related service must not be in competition with the original connected product or related service, according to Article 4 (10) DA.

In principle, the data holder should build the product or service to grant a sort of “accessibility by default and by design” principle, which is analogue to the “privacy by design and by default” principle in Article 25 GDPR. The data holder needs to grant access to the product data and related service data so that the user can access it freely, according to Article 3(1) DA. Furthermore, the data holder must, as a set of pre-contractual duties, inform clearly and comprehensibly about the qualities of data and data-cycle investing product generated data (Article 3(2) DA) and related services data (Article 3(3) DA).

³³ The rules for this case are set in DA’s Chapter V but we are not going to discuss them in this research paper, in particular Arts 14–22 DA.

If direct access to product and related service data is not possible, the user must send an electronic request form to the data holder. However, according to Article 4(1) DA, the data holder is obliged to make data available, including the metadata. According to the same article, there is a parallel between how a data holder and a data controller must give access to data according to Articles 12–15 of GDPR. In the DA context, Article 4(1) obliges the data holder to provide data to the user “without undue delay, of the same quality as is available to the data holder, easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, continuously and in real-time.”

In line with the proposal, according to Article 4(5) DA, the data holder cannot ask for a disproportionately high amount of information to identify the user and also take advantage of it to infer information about its economic situation, according to paragraph 13 of the same article.

DA includes an extended list of mutual duties and obligations of the parties, to rules concerning intellectual property protection and the right to lodge a complaint. The contract between the data holder and the user is the tool through which reciprocal duties and obligations are listed. Both users and data holders may contractually restrict or prohibit accessing or further the sharing of data if, in this way, one can undermine the security requirements of the object, according to Article 4(2) DA. Further, a data holder's duty is not to make the exercise of users' rights difficult by using certain designs while suggesting options, according to Article 4(4) DA. Conversely, the user can't take advantage of gaps in the data-holder technical infrastructure, designed to protect data from being accessed.³⁴ By setting duties of de facto good faith between the parties,³⁵ Articles 3 and 4 DA seem to imply that both the user and the data holder have the same contractual and negotiation power, especially as far as intellectual property, such as trade secrets, are concerned. This is confirmed by Article 13 DA, which sets the non-binding character of a contract as the clause if “its use grossly deviates from good commercial practice in data access and use, contrary to good faith and fair dealing.” Regarding intellectual assets protection, it is highly likely that by giving access to data and metadata, one might expose intellectual property rights such as trade secrets.

The last set of obligations concerns the right to lodge a complaint, defined in paras 3 and 9 of Article 4 DA. The paragraphs are similar in content, but the first refers to disagreements concerning the security restrictions mentioned in Article 4(2), while the second concerns the protection of trade secrets. In both cases, the right to lodge the complaint can be done by following the procedure in Article 37(5)(b) DA or by agreeing with the data holder to solve the issue with a dispute settlement body described in Article 10(1) DA.

The last relevant element is Article 4 DA's explicit connection with data protection concerning the legal basis when the personal data collected are not the user's.³⁶ The paragraph limits itself to pointing out that Articles 6 and 9 GDPR are left unprejudiced, as well as Article 5(3) of the E-privacy directive.³⁷ In connection with practical scenarios involving IoMT stakeholders, this aspect will be dealt with in-depth in Section 3.3 (Fig. 1).

³⁴ Art 4(11) DA.

³⁵ The term good faith in this context is used as the respect of each other's party and the commitment to be fair in executing the contract. It does not have an immediately corresponding translation in English but can be loosely indicated as fairness.

³⁶ Article 4(12) DA. More on the interpretation of this paragraph in relation to the IoMT see *infra* 3.3.

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

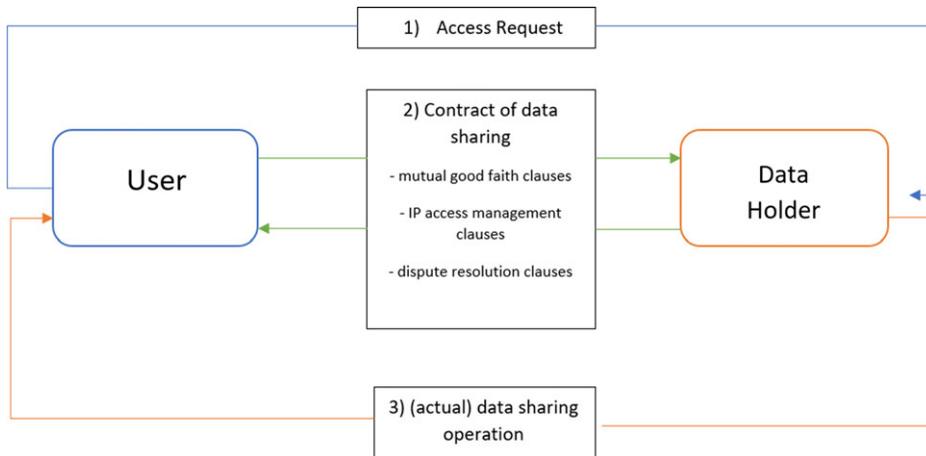


Figure 1. The first data-sharing contract scheme. User – Data holder

(ii) *Data holders, data recipients, user(s) and third parties. Triangular relationships.* The second data-sharing scheme is more complex. According to Article 5 DA, the user can “share data with third parties.”³⁸ Article 5 DA describes two different sub-sets of data-sharing contracts corresponding to the dual definition of the term data recipient analysed in (a).

Article 5(1) DA describes the first subset of data-sharing contracts. In this first hypothesis, the user can ask the data holder to make data available to a third party/data recipient of their choice.³⁹ The alternative, instead, is that a data recipient/third party asks to get access to product/service-related data on behalf of the user to the data holder.⁴⁰ According to the definition of data recipient, there might also be another hypothesis, ie when the third party asks the data holder to get access to the data based on a national or EU law obligation. This last hypothesis seems to be connected to Chapter V, which mandates making data available to public sector bodies, the EU Commission, the ECB and the Union bodies in case of an exceptional need.⁴¹

One of the differences between the articles concerns a subjective prohibition. Article 5(3) DA makes it impossible for the user to designate a gatekeeper within the meaning of the Digital Markets Act (DMA).⁴² This is because whatever platform, cloud service provider, or another one from the list of stakeholders responds to the criteria of Art. 3 DMA, holds such an economic and technological power that it would take advantage to become a

³⁸ It seems that in this case, the terms data recipient and third party are used interchangeably. This can be inferred by the fact that Art 5 DA mentions third parties, while Art 8 DA, referring to the latter, address the “conditions under which data holders make data available to *data recipients*” (italics by authors). This lack of a clear distinction between the two types of actors may impact the future application of these rules in data-sharing contracts. According to Art 2(14) DA, third parties are one of the subjects who could be data recipients, but this definition is not completely overlapping. Who can third parties be, except for parties chosen by the user? Despite this ambivalence, the terms data recipient and third party are used interchangeably for methodological reasons and to avoid confusion.

³⁹ Art 5(1) DA first part.

⁴⁰ *Ibid*, second part.

⁴¹ That is an option that national and the EU administration can use only in a handful of cases which are better detailed at Art 15 DA.

⁴² Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance) PE/17/2022/REV/1 OJ L 265, 12.10.2022, p. 1, available at <<http://data.europa.eu/eli/reg/2022/1925/oj>>.

leader in secondary markets for connected products or related services while already being de facto dominant concerning certain connected products or related services.

Apart from these sub-sets of other contracts, Article 5 DA is similar to Article 4 DA regarding the mutual sets of “good faith” obligations between the data holder and the third party/data recipients. These are, for instance, the third party’s duty to respect the intellectual property assets (trade secrets) of the data holder.⁴³ But the third-party/data recipient also has a set of obligations towards the user set in Article 6 DA. Moreover, only if there is a data recipient can the data holder ask the data recipient to pay a fee, which will need to be calculated according to the fair, reasonable and non-discriminatory (FAIR) principles and exclusively in B2B contracts.⁴⁴

The remaining question concerns the contracts between the user and the third party/data recipient. In the first part of Article 5 DA, it is implicit the conclusion of a contract concerning the fair use of the data holder’s data between the user and data recipient for the creation of the new IoMT pre-exists the contract/agreement between the data holder and the data recipient. The content of this latter contract, described *supra*, includes mutual fairness clauses in the execution of the contract, clauses concerning IP and eventual restrictions of data sharing and dispute resolution clauses. However, one can also imagine the contract’s content that must exist between the user and the data recipient, even though it is not explicitly described in the DA. It might be similar to the data-sharing contract in some ways, but there are at least two different elements. The first set of these specific clauses is the project of the new IoMT or related service characteristics. Almost certainly, there might be clauses concerning IP rights management (eg, whether to try to patent a solution or not to keep it as a trade secret or to make a hypothetical AI-based medical software solution open-source). Moreover, if needed, there could be clauses concerning dispute resolution involving international private law rules. The second set of clauses pertains only to the second kind of contract described by Article 5, where the data recipient directly contacts the data holder for the data-sharing operation. Nevertheless, not only a previous contract on the realisation of the new IoMT or service might already exist between the user and the data recipient/third party, but also a mandate/representation contract. This can also exist in a separate document, but it will contain the formal authorisation of the user to the data recipient to ask the data holder to access the relevant data. It will be up to the national law to govern the rules of this contract of mandate/representation.

To sum up, these subsets of contracts hint at a triangular relationship (data holder, data recipient and user), but they all involve at least two separate contracts in which only two of the parties are directly involved. In the first hypothesis, there is a contract/request by the user to make data available to a data recipient/third party and a contract/set of mutual duties between the data recipient and the data holder as well as, most probably, a contract between the user and the data recipient. In the second hypothesis, the user delegates (through a contract) the third party/data recipient to ask a data holder for access to data. Even in this case, there should be a contract existing between the data holder and the data recipient acting on behalf of the user of which the user is not formally part (Figs. 2 and 3).

3. Overlaps and clashes with data protection framework

After presenting the data-sharing contracts, it is important to verify how the different actors can be qualified according to the GDPR framework.⁴⁵ Despite the DA affirming that it

⁴³ Art 5 (7), (8), (9), (10) DA.

⁴⁴ Art 9(1) DA.

⁴⁵ Note that the reference is redundant, as the GDPR legal framework would have applied to such data processing anyhow.



Figure 2. The second data-sharing contract scheme. User’s request – Data holder

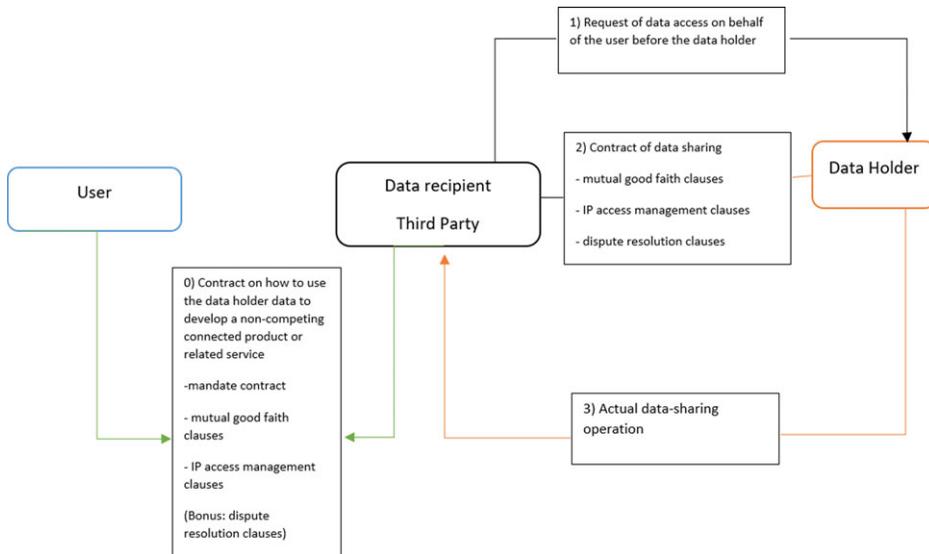


Figure 3. The second data-sharing contract scheme. User’s request to the Data Recipient/Third party

safeguards the application of the GDPR,⁴⁶ also sharing some of its definitions,⁴⁷ there are doubts about the coordination between the GDPR and the DA. The EDPB and EDPS already characterised this relationship as potentially problematic in their joint opinion of 2022.⁴⁸

⁴⁶ Recital 7 DA.

⁴⁷ Such as the definition personal data at Art 2(3), processing at Art 2(7) and data subject at Art 2(10) DA.

⁴⁸ EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act) available at <<<https://edpb.europa.eu/our-work-tools/our-docu>

For IoMT device manufacturers, it is more useful to understand whether there is an overlap (even a partial one) between the GDPR's and DA's subjects not only for compliance reasons but also to understand better how to coordinate these two legislations and, if possible, to simplify the compliance process.

The DA's user definition can partly overlap with GDPR's data subject one. This is because the user can ask to access data that the product or the related service has collected and processed about themselves and other people. Starting from the data-sharing contract between the user and the data holder without an intermediary, in this case the user is generally the one who purchased, rented, leased or, in any case, has an immediate availability of the connected product or the related service and uses it (eg for therapeutic purposes). If the user is a (tech-savvy) consumer and a patient using the IoMT, they can ask the data holder to make the data of their connected product or related service available. The kinds of data the consumer/patient/user can get access to are personal data (such as data related to health or biometric data), non-personal data (such as the logs connected to the functioning and activity of the product or related service), and the connected metadata. If the consumer/patient/user is the only one using the connected product or the related service, the personal data they get access to would be their own, and there are no data protection issues provided that the legal basis they have agreed on to have their connected product/ or related service process their data is lawful. An example is a patient who purchased a rehabilitative connected prosthetic limb (connected product) or who needs to use some exergames based on augmented reality for rehabilitation. In this case, there would be no need to worry about Article 4(12) DA concerning the GDPR legal basis as the user is the only data subject involved. Article 4(12) DA needs to be applied in the case of the user/patient/consumer only if someone else used the device.⁴⁹

There is a significant difference, instead, for the application of Article 4(12) DA if the user is a professional. The case could be of a doctor or a university hospital using a medical device, which could be a connected product (IoMT) or a related service. Let us take the example of a CAT-SCAN operating in a hospital on multiple people every day per year. In this case, both the data holder and the user are already joint controllers under Article 26 GDPR for the data processing linked to the healthcare service.⁵⁰

When looking at the data processing envisaged in the DA, the role of the data controller could be shared among different subjects. The first data controller in chronological order is the data holder. The data holder can be the manufacturer of the connected product,⁵¹ as well as the provider of the related service.⁵² Then, as far as Article 4 DA is concerned, the user can become a data controller for this further processing operation. If the user is a professional, to ask for the re-use of personal data, they will need a legal basis according to Articles 6 and 9 GDPR. Depending on the contractual strength of the user and the context of the data sharing contract, it is not to be excluded that the user can become a joint controller of data according to Article 26 GDPR. Following the previous example, the data

[ments/edpb-edps-joint-opinion/edpb-edps-joint-opinion-22022-proposal-european_en](#)> (last accessed 30 May 2024).

⁴⁹ In the previous example, the users' children may be bored and decide to play the AR exergames because they can't go out to play. If there is a need to log any personal data (name, surname) or if there are connected sensors which can feel the difference between the user and their kids, Art 4(12) DA would apply. In this case, because children are minors, there wouldn't be to consider only Arts 6 and 9, but also Art 8 GDPR concerning minors' consent, with all its different national implementations.

⁵⁰ In fact, the data holder (manufacturer) would need to include a specific clause for their patients in the privacy information document by specifying which legal basis is needed for this specific form of data processing. Similarly, also the hospital will need to assess the GDPR legal basis for the data processing. Being health data, Art 9 (2) GDPR will be the main legal basis.

⁵¹ See Art 3 (2) DA.

⁵² See Art 2(6) DA.

gathered from the CAT-SCAN can help the university hospital researchers to develop a new and more performing software for IoMT software to recognise specific kinds of cancer.

In the case of Article 5, things are more complex as the third party/data recipient is added as a new data controller for further data processing activity. The data holder coincides with the original data controller according to the GDPR. Regardless of whether the data-sharing request comes either from the user or the data recipient/third party with the user's authorisation, the data holder needs to alert all their data subjects (including the user) of the further processing of their personal data, which can be lawful only if based on Articles 6 and 9 GDPR and on the national implementation laws concerning the lawfulness of secondary use of health data. More nuanced is the position of the data recipient/third party. In Article 5 first part, the data recipient/third party comes into play after the formal request that the user has made. Nevertheless, the only contract regulated by the DA will be a data-sharing contract between the data holder and the data-recipient/third party. The data-sharing contract will give the data recipient the role of data controller. Then, the third party and the user can become joint controllers depending on the contract that will be set up to develop a new IoMT or related service and how much the user will be involved in the creation of the new product or service. This is even more likely when thinking about Article 5 second part. In this case, the data recipient contracts with the data holder after receiving the user's mandate/representation contract. What could be the factors for a user to opt for Article 5 first or second part to represent their interests best, if not the technological capabilities and economic strength of the data recipient/third party? In both cases, the user will not directly control the data collected by the data recipient/third party.

If the user is also a data subject (eg a patient), there will be two coordinated activities regained the data processing. First, the user/data subject includes in the mandate contract to the data recipient/third party their consent to the processing of their personal data. Second, the data holder will also have to ask the user/data subject for their consent for the further processing of their data based on Articles 6 and 9 of GDPR and the national authorities' interpretation of the secondary use of health data.

Another aspect to clarify is the position of the professional user (the university hospital to continue with the same example) towards the data subjects, which will need to decide whether to consent or not to further data processing. In case the privacy policy of the professional user does not encompass this specific kind of secondary use, the professional user might use the legitimate interest basis.⁵³ Otherwise, if it is a private entity, it will have to contact again the data subjects which might be using the IoT. This further data processing coincides with the data sharing contract in DA's terms, which the user will not be part of, according to Article 5 DA. According to Article 4 DA, qualifying the professional user in GDPR terms might be easy. Keeping the examples of a contract between a university hospital and a manufacturer. In this case, the hospital is already the data controller of at least some categories of personal data of the data subjects/patients. In this case, it might need to update its privacy policy and clarify which kinds of secondary uses can carry on with patients' data. For this reason, it might include personal data extracted from IoT devices that are lent to patients for rehabilitation purposes (Table 1).

IV. The data-sharing through the European Health Data Space framework

The constellation of actors presented above is not completed, as some additions should be made based on the recent proposal for a European Health Data Space (EHDS).⁵⁴ The

⁵³ Art 6 (1)(f) GDPR.

⁵⁴ Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, COM (2022) 197 final. The European Parliament adopted the document on 24 April 2024. However, it still waits for the approval of the Council. The analysis provided in this contribution is based on the latest version of the

Table 1. Translating the DA framework according to the GDPR interactions.

Actors involved in the data sharing/ Contracts involving data processing	Contract between Uc and DH (Art. 4 DA)	Contract between Up and DH (Art. 4 DA)	(Mandate by Uc) contract between DR and DH (Art. 5 DA)	(Mandate by Up) contract between DR and DH (Art. 5 DA)
User – consumer (Uc)	Data subject (Data controller only if other personal data are shared)	Data subject	Data subject	Data subject
User – professional (Up)	NA	Data controller or joint controller	NA	Third party or Joint controller
Data holder (DH)	Data controller	Joint controller	–	–
Third-party/data recipient (DR)	NA	NA	Data controller	Data Controller or joint controller

regulation aims to provide “a common space where natural persons can easily control their electronic health data. It will also make it possible for researchers, innovators and policymakers to use this electronic health data in a trusted and secure way that preserves privacy.”⁵⁵

As mentioned above, the EHDS regulation does not aim at amending and substituting the GDPR legal framework for health data. In the project of the European Commission, the EHDS aims at adapting and interpreting the GDPR to the specific needs and challenges of health data. In particular, the EHDS regulation seeks to complement the rights provided by the GDPR, addressing two main perspectives: first, the primary use of health data, where the provisions seek to facilitate the reuse of health data by consumers, ensuring portability across health service providers and increasing competition among service providers. The proposal introduces several improvements regarding health data management, such as the design and development of electronic health registries and the interoperability of electronic health record systems across the EU. Moreover, the EHDS Regulation envisages a set of rights for the data subject concerning their personal electronic health data, particularly the right to access “immediately [. . .] free of charge and in an easily readable, consolidated and accessible form.”⁵⁶ To enhance the possibility of achieving the primary use of data and, in the case of cross-border services, the regulation mandates the European Commission to establish a central platform for digital health to provide services and facilitate the exchange of electronic health data.⁵⁷ This approach would overcome the difficulties that emerge in the provision of cross-border healthcare and the fragmented digital standards applicable to health services granting the possibility to data subjects to access their own electronic health data.⁵⁸

Second, the EHDS regulation establishes the legal framework for the secondary use of health data in the EU. It should be underlined that Article 71 EHDS allows the possibility for natural persons to opt out of the secondary use of health data, thus potentially reducing the relevance of the data set made available from data holders. Still, the possibility to access the available data is an added value provided by the procedure set up by the EHDS. Moreover, the secondary use of electronic health data is linked to different purposes, ranging from scientific research to the innovation of new products or services. Article 53 EHDS lists six potential justifications for processing health data for secondary purposes, though not all are uncontroversial. In line with the main focus of this article, the following sections will focus on the rules the EHDS lays down for the secondary use of health data.

One of the first discrepancies emerging when looking at the definitions provided by the EHDS and the GDPR is the one of health data. The type of data covered by the EHDS proposal is wider than the definition of health data given in Article 9 GDPR.⁵⁹ The data covered include both data that squarely fall into the category, such as electronic health records, genomic data and data on patient’s clinical records, but also include other categories of data that only indirectly can be qualified as data that only indirectly refer to

Proposal adopted by the European Parliament, available at <https://www.europarl.europa.eu/doceo/document/TA-9-2024-0331-FNL-COR01_EN.pdf>.

⁵⁵ *Ibid.*, p 1. Note that the European Data Space is the first data space established by the European Commission, and it will probably be the blueprint for a series of similar interventions in other market sectors. See the overall strategy in European Commission, Staff working document on data spaces, 2023, available at <<https://digital-strategy.ec.europa.eu/en/library/staff-working-document-data-space>>.

⁵⁶ Art 7(1) EHDS Regulation.

⁵⁷ Art 23 EHDS Regulation.

⁵⁸ T Petrocnik, “Health Data between Improving Health(Care) and Fuelling the Data Economy” (2022) 2022 Technology and Regulation 124.

⁵⁹ See above para 3.

health,⁶⁰ such as the “data on factors impacting on health, including socio-economic, environmental and behavioural determinants of health” as well as “healthcare-related administrative data, including dispensation, claims and reimbursement data” and also “data from wellness applications” as well as “aggregated data on healthcare needs, resources allocated to healthcare, the provision of and access to healthcare, healthcare expenditure and financing”.⁶¹ For instance, regarding data generated by wellness devices, it may be possible that these data can become health data if they are processed to identify specific health conditions or if they are processed together with other data concerning health.⁶² An example would be the data collected by a wellness device regarding the physical activity of an individual that may become health data if they are connected with the medical prescriptions of a doctor regarding strategies to reduce the level of cholesterol. As is underlined by an evaluation of the proposal by the EDPB and EDPS,⁶³ the quality requirements and characteristics of the health-related data generated by wellness applications are lower than those generated by medical devices.

This wide concept of health data is crucial for the secondary use of data,⁶⁴ which should follow a specific process. A preliminary step is the creation of the national dataset catalogue⁶⁵ that includes the source and the nature of the electronic health data hosted by entities that offer services or perform research in the health or care sector and qualified as health data holders in the regulation. In this case, the definition covers both public bodies, such as hospitals, research centres, and agencies, as well as developers and manufacturers of IoMT and wellness applications.⁶⁶ The body in charge of receiving this information and setting up the national dataset catalogue is the newly created Health Data Access Body (DAB). The DAB is an independent authority set up at the national level⁶⁷ to moderate access to such datasets for health data users.⁶⁸ Health data holders must inform the DAB at the national level, following the rules regarding the minimum information elements describing their datasets.⁶⁹ This first part of the procedure also considers the intellectual property rights and trade secrets that may apply to the datasets: Article 52 EHDS Regulation requires that DAB shall take measures to protect the rights of the health data holders. The legal basis for the data processing carried out by the data holder to share the

⁶⁰ Electronic health data included in the EHDS may be both personal and non-personal data, as some of the information collected does not relate to an identified or identifiable natural person (pursuant Art 4(1) GDPR).

⁶¹ Art 51 EHDS proposal lists seventeen categories of data that can be collected. These categories of data are the ones that the data holders are obliged to make available for secondary use. For a critical analysis of the definition of health see R Rak, “Anonymisation, Pseudonymisation and Secure Processing Environments Relating to the Secondary Use of Electronic Health Data in the European Health Data Space (EHDS)” (2024) 15 European Journal of Risk Regulation 928.

⁶² Wellness applications are qualified as “any appliance or software intended by the manufacturer to be used by a natural person for processing electronic health data specifically for providing information on the health of individual persons, or the delivery of care for other purposes than the provision of healthcare”, see Art 2(2)(ab) EHDS Regulation.

⁶³ EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space, 12 July 2022, p 12, available at <https://edpb.europa.eu/system/files/2022-07/edpb_edps_jointopinion_202203_europeanhealthdataspace_en.pdf>.

⁶⁴ Note that recital 56 EHDS Regulation expressly justifies this approach, affirming that the data processed for secondary use “should be broad and flexible enough to accommodate the evolving needs of health data users” P Terzis, “Compromises and Asymmetries in the European Health Data Space” (2022) 30 European Journal of Health Law 345.

⁶⁵ Art 57 (1) (j) (i) EDHS Regulation.

⁶⁶ Art 2(2)(y) EHDS Regulation.

⁶⁷ Art 55 EHDS Regulation.

⁶⁸ Note that in the case of non-personal electronic health data, the data holder has the ability, through the control of the technical design of a product and related services, to make available certain data to the data user directly, pursuant Art 2 (2)(t)(ii) EHDS Regulation.

⁶⁹ Art 75(12) EHDS Regulation allocates the responsibility to identify such minimum information elements on the Commission through implementing acts.

data with the DAB is Article 6 (1)(c) GDPR, namely the fact that the “processing is necessary for compliance with a legal obligation to which the controller is subject.” At the same time, the EHDS also fulfils the requirements set for health data processing, namely Articles 9 (2) (i) and (j), as the processing is necessary for archiving purposes in public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law.⁷⁰

The second step in the procedure is the data request by the health data users. It must be underlined that the health data user definition does not converge with the user definition in the Data Act, as the EHDS defines health data users as any natural or legal person who can justify access to electronic health data for secondary use. They can submit two types of requests: a data request or a data access application, which should be based on the purposes listed in Article 53 EHDS Regulation.⁷¹ The difference between the two types of requests lies in the type of data that can be accessed. After a health data request, the health data user will receive from the health data holder the anonymised and statistical version of the data,⁷² without providing access to the data that have been used to answer the request.⁷³ In the second case, the data access application will be reviewed by the DAB, which will be in charge of deciding whether or not to grant access to the data and issue – in the affirmative case – a so-called data permit.⁷⁴ Here, the data user should also justify its request upon a legal basis among the ones in Article 6 (1)(e) and (f) GDPR, namely, the data processing is carried out in the public interest or for the purpose of the legitimate interests of the controller. In the first case, the EHDS indicates that the health data user should reference another EU or national law mandating the data user to process personal health data to comply with its tasks.⁷⁵ In the case of a data access application, it will be the data permit issued by the DAB that will define the conditions for the access, namely the types and format of electronic health data accessed, the purpose for which data are made available, the duration of the data permit, the technical conditions for the secure processing environment, as well as the fees to be paid by the health data user.⁷⁶

When the data permit is issued, the data user will coordinate with the DAB to access the data through a secure processing environment without data leaving that repository.⁷⁷ The health data user will become the controller, while the DAB will act as a data processor for the data made available under a particular data permit.⁷⁸

As a result, the process for managing health data in case of secondary use follows the steps presented in Fig. 4.

⁷⁰ Recital 52 EHDS Regulation.

⁷¹ Note that Art 53 EHDS Regulation lists the following purposes: activities for reasons of public interest in the area of public and occupational health; policy-making and regulatory activities to support public sector bodies to carry out their tasks; to produce official statistics related to health or care sectors; education or teaching activities in health or care sectors; scientific research related to health or care sectors, including both development and innovation activities for products and services, and training, testing and evaluating of algorithms, including in medical devices, in-vitro diagnostic medical devices, AI systems and digital health applications; improving delivery of care, treatment optimisation and providing healthcare.

⁷² Article 69(1) EHDS proposal.

⁷³ Article 69 EHDS Regulation requires a set of information to be included in the application, such as a detailed explanation of the intended use of the electronic health data, a description of the requested electronic health data, their format and data source, a description of the statistic’s content, a description of the safeguards planned to prevent any misuse of the electronic health data, a description of how the processing would comply with Articles 6(1) GDPR.

⁷⁴ Article 68 EHDS Regulation.

⁷⁵ Recital 52 EHDS Regulation.

⁷⁶ Art 67 EHDS Regulation.

⁷⁷ Art 73 EHDS Regulation.

⁷⁸ Art 74 EHDS Regulation.

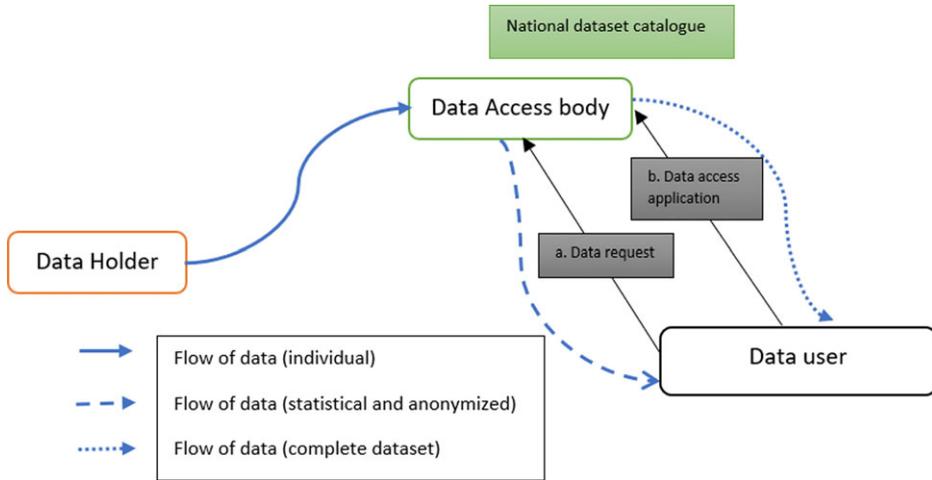


Figure 4. The data-sharing on the basis of EHDS

If we translate this process in the context of the IoMT, we need to clarify if and how manufacturers of the medical devices (or software) fall in the category of data holders and eventually can also qualify as potential health data users. As mentioned above, the definition of health data holders is broad enough to cover not only medical device manufacturers but also many other health applications that do not squarely fall into the “entities performing research” yet collect health data that can potentially support such research.⁷⁹ Thus, in principle, manufacturers of medical devices will be qualified as data holders and required to share their datasets with the DAB.

Looking at the side of the data user, the definition is even wider, as it only requires that the natural or legal person can fulfil one or more of the purposes listed in the aforementioned art. 53 EHDS proposal, without requiring that the data user belong to the sphere of healthcare. It is clear that the manufacturers of IoMT will be able to justify the purposes described in Article 53 (1) (e) (i) and (ii) EHDS. For instance, the purpose of training, testing and evaluating algorithms already refers to the application in medical devices, AI systems and digital health applications, contributing to public health or social security.

According to the definitions, a manufacturer seeking to develop an IoMT can fill a data access request to use the data previously collected by a different data holder, for instance, to train the algorithm used in the IoMT.⁸⁰ Thus, the data access request could avoid the need for the manufacturer to ask the consent of each data subject, as well as the need to identify a specific project to fit the conditions defined for the application of the “research exemption” already provided in Article 9 (2) (j) GDPR as legal basis.⁸¹

⁷⁹ P Terzis, “Compromises and Asymmetries in the European Health Data Space” (2022) 30 *European Journal of Health Law* 345.

⁸⁰ Note that in this case, the EHDS does not include any prohibition for the development of directly competing products, such as the one included in the DA.

⁸¹ According to Art 89 GDPR, the processing for scientific research “shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.” Note that these safeguards are not defined and may be subject to interpretation, see C Staunton and Others, “Appropriate Safeguards and Article 89 of the GDPR: Considerations for Biobank, Databank and Genetic Research” (2022) 13 *Frontiers in Genetics* available at <<https://www.frontiersin.org/articles/10.3389/fgene.2022.719317>> (last accessed 18 January 2024).

Table 2. Translating the EDHS framework according to the GDPR interactions.

Type of processing /Actors involved	Disclosure of data for dataset catalogue	Preparation of dataset catalogue	Making available data upon data access application	Secure processing of pseudonymised data
Data holder	Data controller	–	–	–
Data user	–	–	Data recipient	Data controller
DAB	Data recipient	Data controller	Data controller	Data controller

Given the risks that may be associated with the secondary use of data,⁸² the safeguards included in the EHDS should be strictly applied. In particular, the monitoring role of the DAB will be crucial. The evaluation of the data access application will require not only a mere formal check of the purpose of the secondary use among the ones listed in Article 34 EHDS, but also a substantial analysis of the documentation required in Article 45(2) EHDS.

Unlike the DA's previous analysis, the EHDS does not envisage specific contractual agreements between the health data holder and the health data user.⁸³ The relationships among the actors involved are defined by the regulation itself, relying in any case on the GDPR framework. If we focus on the processing activities, Table 2 clarifies the role of each actor.

V. Conclusions

This article aims to map the options available to manufacturers and researchers to develop new IoMT thanks to the new legislative framework provided by the Data Act and the European Health Data Space Regulation. These legislations start from the shareable assumption that the new medical and health devices can be designed, trained and developed by analysing and processing existing datasets. These activities imply that data will be accessed and transferred from the initial data controller to a data user. In order to protect personal data within this framework, additional rules and processes are envisaged by the DA and the EHDS.

Although data-sharing opportunities were not excluded from the pre-existing legal framework, provided by the GDPR and the MDR, the rules applicable were deemed by the European bodies as hampering innovation. Therefore, the DA and the EHDS were put forward providing alternative options that could enhance the possibilities for research and innovation.⁸⁴

⁸² L Marelli, G Testa and I Van Hoyweghen, "Big Tech Platforms in Health Research: Re-Purposing Big Data Governance in Light of the General Data Protection Regulation's Research Exemption" (2021) 8 *Big Data & Society* 20539517211018783; Terzis (n 78); Slokenberga (n 24); S Slokenberga, O Tzortzatou and J Reichel (eds), *GDPR and Biobanking: Individual Rights, Public Interest and Research Regulation across Europe*, vol 43 (Springer International Publishing 2021) available at <<https://link.springer.com/10.1007/978-3-030-49388-2>> (last accessed 25 August 2023).

⁸³ The exception is the case of contractual agreements addressing the data containing information or content protected by intellectual property rights or trade secrets. This hypothesis is envisaged in Art 51 (4) EHDS Regulation, where it is also specified that the Commission may recommend non-binding model contractual terms for such arrangements.

⁸⁴ Although both legislations are regulations directly applicable in the Member States, national adaptations will still be relevant in order to evaluate if and how data sharing will be achieved. Similarly to what has happened in the interpretation of Art 29 GDPR by national data protection authorities, national specificities may reduce or facilitate data sharing activities, for instance, depending on the approach of the Data access body vis-à-vis the legal basis used by data users to justify their data requests.

Before detailing the pros and cons of the DA and the EHDS sharing processes, it is worthwhile to point out some similarities. The first one is *ratione materiae*: the EHDS and the DA can apply to the same sets of objects. IoMT devices are bound to become increasingly used in hospital and home environments. Another similarity is the centrality of the data holder, which is the first data controller according to the GDPR. This role affects the tasks and obligations of the data holder both in the EHDS and the DA. Under the DA, the data holder is the addressee of the request of the user and, at a later stage, the data recipient/third party.⁸⁵ In the EHDS, the data holder is obliged to make its dataset to the Data access body. Then the data user's request to the data access body prompts the latter to transfer or allow access to the data requested to the data user. In both legislations, the data holder the point of reference for the secondary use of data.

When it comes to differences, they relate to the purposes for which an actor asks to have access to data and the means through which the transfer operation occurs.

According to the EHDS, the primary purpose of secondary use of data is research and, eventually, the development of medical and non-medical devices (ie, wellness apps not certified as MD). This justifies access to a much larger amount of data that can be made available to corroborate scientific research. This quantity of data is essential to design IoMT because the MDR requires medical devices to have clinical evidence that they are safe and do not harm patients through clinical data.⁸⁶ Another characteristic is that the EHDS provides for a more centralised procedure subject to administrative control. The administrative bodies in charge of exercising the tasks of the DAB require implementation by the states and coordination that will probably be slowed down in the early stages of application. The EHDS will likely require more years than the ones specified in the act for the transition to its full implementation. Once implemented, it will give easier access to more data than the DA.

Conversely, the DA has the function of horizontal regulation and has the purpose of creating IoT devices in general but also IoMT devices, given that there is no specific legislation on IoMT yet, and there will, probably, not be one in the future. Among the positive features of this legislation is the decentralised approach, stemming from the autonomous initiative of private actors or even public actors whenever acting with a private actor's logic (eg, a university hospital which wants to develop a new IoMT or related service through its research teams). The main characteristic of the DA is the regulation through contracts. This is, in principle, a more flexible process than the administrative based one, ie, the EHDS one. However, the fact that everything is regulated through contracts might also add some difficulties in making the market truly competitive and enacting the principle of the free flow of data. Despite Article 13 DA affirms the invalidity of the unfair clauses, the drafting and the management of all these (almost) triangular relationships will be a hidden cost that not many users or third parties might be able to sustain, especially if the IoMT device is produced by an important medical device manufacturer. This unbalance could also emerge in the IP rights obligations that the user or third party/data recipient must abide by. Moreover, the user or third party must have access to several IoMTs or have the availability of an IoMT, which creates a considerable amount of data, to gather a sufficient amount of data to identify patterns and train an algorithm. Another variable which might negatively impact the success of the DA depends on the market strength, respectively, of the data holder, user and third party. The combination of the DA rules and GDPR's principles concerning data portability are the only rules that can be applied directly also by IoMT manufacturers that are not dominant on a market and by medical researchers who want to market the result of their studies. Hence,

⁸⁵ Arts 4 and 5 first part DA.

⁸⁶ See above Section 3.

as far as the time of writing, the Data Act is the most complete discipline, together with the GDPR, to be used to bring innovation to the IoMT sector.

Acknowledgments. The authors wish to thank Irene Aprile, Tommaso Crepax, Simona Demkova, Enea Parimbelli, Silvana Quaglino, Arianna Rossi, and Giuseppina Sgandurra for suggestions, comments and access to the repository on medical devices within the Fit4MedRob project. The research was carried out in the framework of the PNRR project “SoBigData.it: Strengthening the Italian RI for Social Mining and Big Data Analytics” (CUP B53C22001760006) (F. Casarosa) and “Biorobotics Research and Innovation Engineering Facilities” (IR0000036” – CUP J13C22000400007) (F. Gennari).

Competing interests. The authors confirm there are no conflicts of interest to declare.