Data sharing and health services in the Italian legal framework: case study

Francesca Romana Pesce

Abstract

Data play a key role in the world economy. This is the reason why regulations should govern such aspect not only restricting and limiting the use of data but also creating opportunities for the re-use of data while removing technical and legislative barriers.

The Data Act fits within the aforementioned scopes. In particular, this paper will focus on the right to share data with third parties (article 5) and provisions related to the interoperability (article 28 ff.). In the data protection field, the health industry is one of the most sensitive and and focused on the public interest. This means that this sector could be one whom benefit the most from an exchange policy of personal data.

Currently, in Italy, all health records issued by a public sanitary structure are made available to the patient within the Fascicolo Sanitario Elettronico (FSE), a digital platform where all health record are stored and accessible by the data subject and health public structure. While public entities are obliged to provide this service and are able to access those data, is not clear if private health structures need to converge within the FSE all the health documentation produced, but certainly are not allowed to access them.

Considering this, this paper will analyze, within the Italian legal framework, opportunities for the right to access (article 15 GDPR) and portability (article 20 GDPR) of health records, requested by an authorized parties in order to be able to secure a private database of health data. Strengths and weaknesses along with risks and opportunities of this project will be analyzed taking into account the legal point of view and some technical aspects.

The aim of this paper is to show how opportunities for the share and re-use of data combined with the removal of technical and legislative barriers provided by new and updated legislation can have a great positive impact not only for the healthcare sector but also for patients.

Index

1. Introduction

Data play a key role in the world economy. This is the reason why regulations should govern such aspect not only restricting and limiting the use of data but also creating opportunities for the re-use of data while removing technical and legislative barriers.

The proposal for a Regulation of the European Parliament and act of Council n. 2022/0047 on harmonized rules on fair access to and use of data (also known as Data Act) fits within the aforementioned scopes. According to the objective of the proposal its aim is to *ensure fairness in the allocation of value from data among actors in the data economy and foster access to the use of data.* In particular, this paper will focus on the right to share data with third parties (article 5) and provisions related to interoperability (article 28 ff.).

In the data protection field, the health industry is not only one of the most sensitive, but also the one with an exceptional need for the performance of a task carried out in the public interest. This means that this sector could be one that benefits the most from an exchange policy of personal data.

Currently, in Italy, all health records issued by a public sanitary structure are made available to the patient within the Fascicolo Sanitario Elettronico (FSE), a digital platform where all health records are stored and accessible by the data subject and health public structure for study and scientific research in medical fields and for health care planning, verification and evaluation and with the patient consent also for diagnosis, treatment, prevention and international prophylaxis. While public entities are obliged to provide this service and are able to access those data, it is not clear if private health structures need to converge within the FSE all the health documentation produced. It is certain, however, that they are not allowed to access it.

Considering this, the paper will analyze, within the Italian legal framework, opportunities for the right to access (article 15 GDPR) and portability (article 20 GDPR) of health records, requested by an authorized parties in order to be able to secure a private database of health data. These kinds of chances are not currently granted by the regulation but both clinical institutions and patients themselves can benefit from it. Strengths and weaknesses along with risks and opportunities of this project will be analyzed taking into account not only the legal point of view by evaluating possible legal instrument required and the possibility of using such methodologies by delegation, but also considering some technical aspects.

The aim of this paper is to show how opportunities for sharing and re-usage of data combined with the removal of technical and legislative barriers provided by new and updated legislation can have a great positive impact not only for the healthcare sector but also for patients.

2. European strategy on data exchange

The new European data strategy focuses on putting people first by promoting European values and rights in the digital world. Its aim is to ensure that the European Union not only becomes a role model and a leader for a society empowered by data but also a secure, attractive and dynamic data-driven economy. Both goals can be achieved by creating a single market data within which data will be able to flow freely within the EU and across all sectors in order to benefit businesses, researchers and public administrations.[1] Data driven applications will also benefit data subjects in many ways such as creating a safer and cleaner transport systems, generating new services and products, improving sustainability and energy efficiency, reducing the costs of some public services and last but not least improving health care.[2]

The President of the European Commission, Ursula von der Leyen, is a strong advocate for European digitalization and for all the benefits that a sharing approach can bring to the actual situation. According to her "*we will need to overcome fragmentation in our single market that is often greater online than elsewhere. We need to join forces – now. Not by making us all the same, but by leveraging our scale as well as our diversity – both key factors of success for innovation […] We will develop a legislative framework and operating standards for European data spaces.*

---

[1] European Commission website, *A European Strategy for data*, available at: <https://digital-strategy.ec.europa.eu/en/policies/strategy-data> (accessed: July 08th, 2022).

[2] *ibidem*

These will allow businesses, governments and researchers to store their data and access trusted data shared by others. This will all be done under secure conditions that create greater value for all and ensure a fair return for all."[3]

Among the European governing bodies, the President Von der Leyen is not the only one with a new and innovative approach on sharing data. The European Council in its Conclusions of 1-2 October 2020, stressed "*the need to make high-quality data more readily available and to promote and enable better sharing and pooling of data, as well as interoperability"*[4]. A concept reaffirmed on March, 25 2021 by underlining "*the importance of better exploiting the potential of data and digital technologies for the benefit of the society and economy"*[5], and in 2021 by highlighting "*the importance of making rapid progress on existing and future initiatives, in particular unlocking the value of data in Europe, notably through a comprehensive regulatory framework that is conducive to innovation and facilitates better data portability, fair access to data and ensures interoperability*".[6]

The journey to the above mentioned project is not brand new, it started a few years ago, and the keys to this goal are Regulations. Starting with the Regulation (EU) 2016/679 also known as GDPR (General Data Protection Regulation), the toughest privacy and security law in the world, put into effect on May 25, 2018.[7] The scope of this regulation was, in fact, to ensure a respectful and compliant *processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.*[8] In order to ensure benefits to all it is also necessary to establish clear and fair rules on data access and reuse and sharing European data in key areas, with interoperable and common data spaces.[9] Those key aspects can be accessed by drafting a legislation that not only restricts and limits the use of data but also creates opportunities for the re-use of data while removing technical and legislative barriers such as the Data Act.

2.1 Data Act

On 23 February 2022, the European Parliament and the Council proposed a Regulation on harmonized rules on fair access to and use of data also known as Data Act. The proposal had been put forward with the aim of ensuring fairness in the allocation of value from data among actors in the data economy and to foster access to and use of data.[10] The Data Act, precisely because of its purpose, is a key pillar of the new European strategy for data. In fact, it enables to exploit the potential of the increasing amount of data to benefit the European economy and society.

In order to realize the above presented goal, the new proposal aims to (i) adopt legislative measures on data governance, access and reuse; (ii) make available more data by opening up publicly held datasets across the EU and allowing their reuse for free; from a more practical point

---

[3] Pub Affairs Bruxelles- EU Debates, News & Opinions website, *Shaping Europe's digital future: op-ed by Ursula von der Leyen, President of the European Commission* available at <https://www.pubaffairsbruxelles.eu/eu-institution-news/shaping-europes-digital-future-op-ed-by-ursula-von-der-leyen-president-of-the-european-commission/> (accessed: July 08th 2022).

[4] European Council, European Council meeting (1-2 October 2020) - Conclusion EUCO 13/20, 2020, p. 5.

[5] European Council, Statement of the members of the European Council meeting (25 March 2021) –Statement SN 18/21, p. 4.

[6] European Council, European Council meeting (21-22 October 2021) - Conclusion EUCO 17/21, 2021, p. 2.

[7] GDPR.EU website, *What is GDPR, the EU's new data protection law?,* available at: <https://gdpr.eu/what-is-gdpr/> (accessed: July 9th 2022).

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation - GDPR), 2016, Art. 2 par. 1.

[9] European Commission website, *European data strategy*, available at: <https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy> (accessed: July 10th 2022).

[10] 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), 2022, pag.2.

of view, (iii) ensure access to fair and secure cloud by facilitating the set-up of a procurement marketplace for data processing services and creating clarity about the applicable regulatory framework on cloud framework; (iv) invest in a European High Impact Project to develop tools, infrastructure and governance mechanisms in order to easily and safely share data[11]. The benefits of this new approach are undeniable, and, as a result of this data strategy, companies will have more data available to innovate and develop. Considering just the Business-to-Government data sharing, The High-Level Expert Group on Business-to-Government Data Sharing appointed by the European Commission, in 2020, published a report highlighting its advantages and proposing a set of policies on the topic.[12]

As previously mentioned, the Data Act is not the only legislation that plays an important role in data sharing. The GDPR is always worth considering in the data field. This is the reason why the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) published, on May 4th 2022, a joint opinion[13] on the compliance of the Data Act in light of the GDPR. According to them there are two aspects worth underlining. The first aspect concerning the EDPB and the EPBS was the use of the relevant data for purposes of direct marketing, employee monitoring, credit scoring and for special categories of data such as data related to the health status of a data subject, calculating, modifying insurance premiums. Secondly, while accessing, using and sharing data in line with the Data Act provision in particular article 5 and 28, it is always important to comply with all data protection principles.[14]

2.1.1 Right to share data with third parties - article 5 Data Act

Article 5 of the Data Act, which focuses on sharing data with third parties, is the core of one of the main aspects of the proposal. This provision in regulating the important aspect of data sharing, enables third parties, except from gatekeepers, authorized by the data subject to make the request on their behalf to the data controller. The only requirement is that they are able to prove their quality as an authorized subject, without hindering, preventing or interfering with the right to data portability under Article 20 GDPR.

According to the first paragraph of that article *upon request by a user, or by a party acting on behalf of a user, the data holder shall make available the data generated by the use of a product or related service to a third party, without undue delay, free of charge to the user, of the same quality as is available to the data holder and, where applicable, continuously and in real-time.*[15] This section was not always so intended. According to the analysis of the leaked draft of the proposal on February 2nd 2022, and the one published on February 23rd. At first the only part allowed to submit a request in order to access data was the data subject. Within the provision later published, the scope of this right has been extended by granting the submission also to a party acting on behalf of a user. Always within the above mentioned provision, it is also specified

---

[11] European Commission website *A European Strategy for data* available at:
< https://digital-strategy.ec.europa.eu/en/policies/strategy-data> (Accessed: July 10th 2022).

[12] High-Level Expert Group on Business-to-Government Data Sharing, *Towards a European strategy on business-to-government data sharing for the public interest,* 2020, available at: <https://www.euractiv.com/wp-content/uploads/sites/2/2020/02/B2GDataSharingExpertGroupReport-1.pdf > (accessed: July 10th 2022).

[13] 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),* 2022, available at: <https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-22022-proposal-european_en> (accessed: July 10th 2022).

[14] EDPB website *The EU's Data Act: data protection must prevail to empower data subjects*, May 5th 2022, available at:
<https://edpb.europa.eu/news/news/2022/eus-data-act-data-protection-must-prevail-empower-data-subjects_en> (accessed: July 10th 2022).

[15] 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), 2022, art. 5 phar. 1

that the data should be made available to the third party in the same quality as is available to the data controller.[16]

Article 5 also sets an obligation of the data holder to make data available to third parties. It states that *any undertaking providing core platform services for which one or more of such services have been designated as a gatekeeper […] shall not be an eligible third party under this Article.*[17] The parties identified by the European Commission do not include the so-called gatekeepers, from the benefitting from these new data sources.[18] The gatekeepers were introduced and defined by the Digital Markets Act as the middlemen between those accessing the Internet and those offering content on the network.[19]

In case the information is requested from a third party, it is specified that the latter *shall not be required to provide any information beyond what is necessary to verify the quality […] as an authorized third party.*[20] This provision demonstrates the influence of the GDPR within any data-related legislation. Indeed, clear reference is made to the need for the data controller to be able to know and ascertain the identity and quality of the applicant as stated in article 12 paragraph 2 of the GDPR.

The above mentioned paragraph in article 5 of the Data Act is not the only one that refers to the Regulation (EU) 2016/679. It is stated that in case of *any failure on the part of the data holder and the third party to agree on arrangements for transmitting the data shall not hinder, prevent or interfere with the exercise of the rights of the data subject under Regulation (EU) 2016/679 and, in particular, with the right to data portability under Article 20 of that Regulation.*[21] The importance to stress of the division and the non-interference between article 5 and the right of the data subjects stated in the GDPR was highlighted also by the EDPB and the EPBS in their considerations. In the same document it also has been recommended reporting into a Recital the criteria to balance the right to portability with data protection concerns related to other persons set out by EDPB in the guidelines on data portability.[22]

Should this provision be approved it would substantially alter what is the current regulatory landscape regarding data sharing. As will be highlighted below, such an article would, in fact, allow for the exchange of data in situations where there are currently countless problems.

2.1.2 Interoperability - article 28 ff

Interoperability is the ability of computer systems or programs to exchange information[23] and as stated in 2010 by the European Comission, in the Digital Agenda for Europe, is considered essential to the development of the digital economy.[24] Even though this aspect is not the main core of the legislation it is certainly essential to its aim. In fact, as previously mentioned, the data sharing provision is the main aspect of the Data Act, but interoperability is the condition without

---

[16] DR2 consultants *ANALYSIS The Data Act proposal from the European Commission*, 2022, available at: <https://dr2consultants.eu/wp-content/uploads/2022/03/Analysis-of-the-Data-Act-proposal-from-the-European-Commission.pdf> (accessed: July 16th 2022).

[17] 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), 2022, art. 5 phar. 2.

[18] C. Perarnaud R. Fanni, *THE EU DATA ACT Towards a new European data revolution?* CEPS Policy Insights, No 2022-05/ March 2022.

[19] Proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (digital markets act), 2020.

[20] 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), 2022, art. 5 phar. 3.

[21] 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), 2022, art. 5 phar. 7.

[22] 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),* 2022, p.15 available at: <https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-22022-proposal-european_en> (accessed: July 16th 2022).

[23] Oxford Dictionary – interoperability, 2022.

[24] EU Commission, A Digital Agenda for Europe, Brussels, 2010, COM, p. 3.

which sharing is, if not impossible, certainly extremely difficult and expensive. In this respect, the Data Act proposes not only a new standardization framework for data and cloud interoperability but also contractual obligations for cloud providers.[25]

In addition to the European Commission also other actors have advocated, researched and studied policies in order to guarantee interoperability among services, platforms and networks.[26] The Data Act has a whole chapter well-articulated and dedicated to interoperability.

In fact, chapter VIII called, *interoperability* aims to secure measures that will enable the commission to guarantee interoperability in detail. Therefore, with this goal in mind the commission was allowed to mandate European standardization organizations to draft standards on the subject; adopt common specifications in cases where harmonized standards are insufficient; and adopt guidelines establishing detailed interoperability specifications, such as architectural models and technical standards. The Data Act, in this way, *offers the opportunity to go beyond the data portability approach introduced by the GDPR, which has proven ineffective*. In fact, the privacy legislation made the right to portability mandatory but did not specify its technical characteristics. This resulted in an inevitable limited adoption of the right and faculty to exchange data.[27]

The core of this chapter is without any doubt article 28 which gives essential requirements regarding this aspect. According to paragraph 1 of the mentioned article 28 *operators of data spaces shall comply with the following essential requirements to facilitate interoperability of data, data sharing mechanisms and services:*

(a) the dataset content, use restrictions, licenses, data collection methodology, data quality and uncertainty shall be sufficiently described to allow the recipient to find, access and use the data;

(b) the data structures, data formats, vocabularies, classification schemes, taxonomies and code lists shall be described in a publicly available and consistent manner;

(c) the technical means to access the data, such as application programming interfaces, and their terms of use and quality of service shall be sufficiently described to enable automatic access and transmission of data between parties, including continuously or in real-time in a machine-readable format;

(d) the means to enable the interoperability of smart contracts within their services and activities shall be provided.[28]

At the beginning the first internal draft of the document did not include article 28 as we know from the proposal published on February 23rd. This is the reason why the first draft failed the internal impact assessment. The Regulatory Scrutiny Boardwas, in fact, considered it too vague on how interoperability, a key aspect on the subject, should be achieved.[29]

As this subject plays a key role in the data economy, besides legislative measures, the European Commission has proposed a number of other initiatives once again related to interoperability between systems. One of the most relevant is Joinup which has been created in

---

[25] European Commission website, *Data Act – Questions and Answers*, 2022, available at: <https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_1114> (accessed: July 17th 2022).

[26] W. Kerber, H. Schweitzer, *Interoperability in the Digital Economy*, 2017, JIPITEC 39 para 1. Available at <https://www.jipitec.eu/issues/jipitec-8-1-2017/4531/?searchterm=None> (accessed: July 17th 2022).

[27] A. Tarkowski, F. Vogelezang in Open Future, *Data Act: Interoperability and Data Sharing services,* 2022, available at <https://openfuture.eu/publication/data-act-interoperability-and-data-sharing-services/> (accessed: July 17th 2022).

[28] 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), 2022, art. 28 phar. 1

[29] T. Schwab, in GED, *Reshuffling the Data Economy: The Major Role Interoperability Plays in the Data Act*, 2022, available at: <https://globaleurope.eu/europes-future/reshuffling-the-data-economy-the-major-role-interoperability-plays-in-the-data-act/> (accessed: July 17th 2022).

order to communicate and collaborate on IT projects across Europe by providing a common venue where public citizens, business and public administrations are able to share and reuse IT solutions and good practices.[30]

3. Case study: sharing special categories of personal data

In the data protection field, the health industry is not only one of the most sensitive, but also the one with an exceptional need for the performance of a task carried out in the public interest. This means that this sector could be one whom benefits the most from an exchange policy of personal data. Currently, in Italy, all health records issued by a public sanitary structure are made available to the patient within the Electronic Health Records (hereinafter FSE),[31] a digital platform where all health records are stored and accessible by the data subject.

According to the recent legislation,[32] public health structures are obliged to provide this service by enriching the FSE with all new data related to the data subject.[33] Along with the obligation to enter new data into the FSE the new legislation also gives them the right to access it for study and scientific research in medical fields, for health care planning, verification and evaluation and, with the patients' consent, also for diagnosis, treatment, prevention and international prophylaxis.[34]

If the position regarding data entry and access for public health structure is well defined as stated above, the same cannot be said for the private ones. Regarding the duty to directly update and enrich the data subject FSE the law is blurry, and it is not clear whether it is mandatory or allowed for private health facilities to do so. Article 12 paragraph 3 of the Law Decree n. 179/2012 as modified by the Law Decree n.4/2022, in fact, states: "*the FSE is enriched with the data of present and past clinical events referred to in Paragraph 1 in a continuous and timely manner, without further burden on public finance, by the individuals and health professions taking care of the assisted person both within and outside the National Health Service and regional social and health services, as well as, at the initiative of the patient, with the medical data held by the patient."*

On the other hand, with regard to the possibility of access, neither within paragraph 5, which governs the possibilities of access for public facilities, nor in any other paragraphs of Article 12 there is any reference to the possibility for private facilities to consult and access the data contained within the FSE.

Santagostino is a network of comprehensive private outpatient clinics founded in 2009.[35] This innovative and creative center, since the beginning has made available to its patients a kind of FSE called *Dossier* in order to obviate the silence and lack of clarity in the regulations. Within each Dossier, each patient, in compliance with the regulations and guidelines in the field of telematic accessibility of health data, can consult and receive his/hers reports. Following, however, the change in the new legislation, Santagostino, still not seeing the possibility for private facilities to access the FSE recognized, requested an opinion[36] from a legal and technical point of view, of the possibility to obtain a proxy from the patient to access the patient's data contained within the FSE in order to enrich the *Dossier*. This would allow the patient himself a

---

[30] European Commission website, *Joinup interoperable Europe* available at: <https://joinup.ec.europa.eu> (accessed: July 17th 2022).

[31] Ministero della Salute website, *eHealth - Sanità digitale,* available at: <https://www.salute.gov.it/portale/ehealth/dettaglioContenutiEHealth.jsp?lingua=italiano&id=5491&area=eHealth&menu=fse> (accessed: July 30th 2022).

[32] Decreto Legge n.4/2022 in emendation of art. 12 Decreto Legge n. 179/2012 available at: <https://www.gazzettaufficiale.it/eli/id/2022/01/27/22G00008/sg> (Accessed: August 1st 2022).

[33] Art. 12 co 3 Decreto Legge n. 179/2012 is modified by Decreto Legge n.4/2022.

[34] Art. 12 co 5 Decreto Legge n. 179/2012 is modified by Decreto Legge n.4/2022.

[35] Santagostino website available at: <https://www.santagostino.it/it/chi-siamo> (accessed: August 3rd 2022).

[36] Annex A.

more effective management of all referrals coming not only from the Santagostino but also from other facilities.

3.1 The risks of data exchange

Certainly, like any data processing, sharing can involve risks. Risks that, due to the nature of the data involved, should not be ignored and should be approached with the utmost caution by observing the provisions on risk limitation and processing of personal data. The most common types of risks are data breaches and legal risks.

Data breach can be categorized according to the following information security principles as: (i) *Confidentiality breach* when there is an unauthorized or accidental disclosure or access to personal data; (ii) *Integrity breach* when there is an unauthorized or accidental alteration of personal data (iii) *Availability breach* when there is an accidental or unauthorized loss, access or destruction of personal data.[37] The above mentioned security threats can have a great impact on companys' assets, reputation and even activities to a point where their competitiveness and ability to innovate are undermined.[38] Digital security incidents are growing proportionally with the intensity of the use of data. The motive for these illegal actions varies from money earned from selling data on the black market to personal and political reasons.[39] Cyber-attacks that, as we know from past experiences, do not spare health centers.[40]

Legal risks, even though they are relatively new with respect to data breaches, are equally important in consideration of the activities of all Europeans Data Protection Authorities (DPA). As mentioned before, while processing data is extremely important to comply with the legislation and to limit and avoid breaches, it is necessary to take into account security measures. The GDPR does not provide a list of necessary measures, but it revolves around a risk approach and the principle of accountability i.e., on the adoption of proactive behavior and such as to demonstrate the concrete adoption of measures aimed at ensuring the implementation of the regulation.[41] Article 32 GDPR, in fact, provides just with a list of some example of security measures that can be adopted or integrated based on *the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons*.[42] Nevertheless, around all Europe in 2021 there have been around 100 violations of article 32 of the GDPR, and this year we can already count 44 violations of the same article.[43]

3.1.1 Risks minimization

---

[37] EDPB guidelines 01/2021, on *Examples regarding Personal Data Breach Notification,* (2021) available at: <https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012021_pdbnotification_adopted_en.pdf> (accessed: August 3rd 2022).

[38] OECD, *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, OECD Publishing, 2019, also available at: <https://www.oecd-ilibrary.org/sites/15c62f9c-en/index.html?itemId=/content/component/15c62f9c-en> (accessed: July 30th 2022).

[39] OECD, *OECD Digital Economy Outlook 2017*, OECD Publishing, 2017, also available at: <https://espas.secure.europarl.europa.eu/orbis/sites/default/files/generated/document/en/9317011e.pdf> (accessed: August 3rd 2022).

[40] NAO - National Audit Office, *Investigation: WannaCry cyber attack and the NHS,* (2017) available at: <https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/> (accessed: August 3rd 2022).

[41] Garante Per la Protezione dei Dati Personali, *Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali*, available at: <https://www.garanteprivacy.it/misure-di-sicurezza> (accessed: August 3rd 2022).

[42] EDPB, Guidelines 4/2019 on *Article 25 Data Protection by Design and by Default*, 2019, available at: <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf > (accessed: August 3rd 2022).

[43] GDPR Enforcement Tracker, available at: <https://www.enforcementtracker.com> (accessed: August 3rd 2022).

As just demonstrated, even though data sharing can bring benefits, it does also involve risks. That is not to say, however, that it is necessary to forego the benefits. In relation to that the ICO proposes a list of steps[44] to be taken in order to ensure safe and compliant processing of health data, always keeping in mind the risk-based approach and the accountability principle at the heart of the GDPR.

Security measures are certainly one of the main aspects that needs to be addressed while talking about risk minimisation. The GDPR, as previously stated, proposes just a few examples of security measures in art 32, as the European Union Agency for Cybersecurity (ENISA) proposes a better and more in-depth analysis of the topic. According to the 2021 ENISA report security measures can be divided into two main categories: technical measures and organizational ones. Technical measure includes (i) develop cybersecurity culture by appoint an internal professional specifically dedicated to the function, conduct audits, and propose customized training courses that focuses on real situations; (ii) deploy a security access to the IT system and device safety by encryption, keeping devices constantly updated and being able to remotely erase data; (iii) guarantee the security of not only the corporate network and website but also the physical corporate one. Organizational measure, instead, includes (i) implement a privacy by design approach; (ii) provide the draft of the documentation required by the GDPR such as record of processing activities, privacy policies and risk assessment; (iii) create an organizational model for the sharing of responsibilities and competences in the field of privacy.[45]

The ICO also proposes other elements, that are referred to in the GDPR, that needs to be considered before starting to process special categories of data such as sanitary ones. Data minimisation is the first suggestion made by the UK DPA. It means that a data controller should limit the processing of personal data to what it is directly and strictly relevant to fulfill a specified purpose. This principle is not only expressed in Article 5(1)(c) of the GDPR but also in Article 4(1)(c) of Regulation (EU) 2018/1725.[46] Transparency is another principle that needs to be taken into account. Stated by article 13 and 14 of the GDPR requires that any information or communication related to the data processing should be clear and accessible. Data subjects should also be made aware not only of their rights but also of the risks related to the processing.[47] In addition to the principles, the ICO has emphasized the importance of documentation and records that need to be maintained by the data controller and the need under article 37 of the GDPR to appoint a data protection officer.

3.2 The benefits of data exchange

Secure data sharing is always followed by countless benefits. Evidence of this is certainly the drafting of new dedicated legislation. The Data Act, as also stated before, considers sharing one of the main aspects to take into account in order to develop a single market for data and to make Europe a global leader in the data economy.[48] International legislation is not the only one that strengthens the importance of data sharing. The Italian legislation by providing in paragraph 11-*bis* of Article 12 of Decree Law n. 179/2012 as amended by Decree Law n.4/2022 the obligation on the part of health care providers to implement the patient's FSE without delay,[49] and the opportunity at paragraph 5 of the same article to access those data not only by the data subject

---

[44] ICO website, *What are the rules on special category data?*, available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-rules-on-special-category-data/> (accessed: July 30th 2022).

[45] ENISA, *Threat Landscape 2021*, 2021, available at: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021> (accessed: August 5th 2022).

[46] European Data Protection Supervisor, Glossary – Minimisation, available at: <https://edps.europa.eu/data-protection/data-protection/glossary/d_en> (accessed: August 3rd 2022).

[47] Data Protection Commission Ireland, *The right to be informed (transparency) (Article 13 & 14 GDPR),* available at: <https://www.dataprotection.ie/en/individuals/know-your-rights/right-be-informed-transparency-article-13-14-gdpr> (accessed: August 3rd 2022).

[48] 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).

[49] Art. 12 co. 11-*bis* Decreto Legge n. 179/2012 es modified by Decreto Legge n. 4/2022.

but alto for the public health structure,[50] clearly highlights the importance of sharing special categories of data such as the one related to the data subject health. Specifically with regard to the issue addressed by this paper, the benefit of data exchange can be approached by two different points of view: the one of the health companies and the one of the patients.

3.2.1 Benefits for health industries

Data is valuable. This is the main reason why the European Union has decided to regulate this very important topic. For companies more data about their customers means having the possibility to provide better and customized service to the needs of the individual. If this customization, although certainly limited and regulated by strict legislation, is permitted for commercial purposes surely, we do not see the reason to exclude it in the health care sector where the object of the service that is sought to be improved is precisely the health of the individual.

More and updated data can support medical research and innovation. Different and similar data if analyzed can give a broader view of the problem allowing a medical structure to develop new health interventions. This could include the possibility for medical staff to research the issue and find faster a special treatment for each patient. The goal is to turn data into knowledge that can be used to improve patient safety, research and innovation. Technologies and data access across different services can also improve the health care system as a whole. To benefit from it would in fact be systems, efficiency and workforce experience. Last but not least, companies can also benefit from empowering patients. Technologies and procedures that allow patients to easily access all their data and thus, enabling them to manage their own health and provide more accurate and specific information to their physicians can guarantee time saving and more accurate visitation.[51]

The above mentioned benefits are probably the reasons that led the High-Level Expert Group on Business-to-Government Data Sharing to draft the final report where "health" is one of the most recurring terms. It is not surprising considering how exchanging data between different health facilities can influence time and money-saving.[52] A kind of advantage that can certainly benefit the patient too.

3.2.2 Benefits for the patient

As pointed out above the benefits for patients are actually closely linked with those of the companies being the aim of the latter to provide the most comprehensive and reliable health service possible. The patient in fact will benefit not only by being empowered but also accessing a better health care system.

The access to patient updated and diverse health data by him and the health company treating him have the power to completely transform patient care. The data can come from different sources such as care homes, public health structure or even reported by patients themselves. This diversity is the key of a more accurate[53] and early diagnosis.[54] An example of all the benefits arising from such a sharing approach is that documented by the High-Level Expert Group on Business-to-Government Data Sharing appointed by the European Commission. Brought up as an example of the importance in data sharing is the case of how a partnership

---

[50] Art. 12 co. 5 Decreto Legge n. 179/2012 es modified by Decreto Legge n. 4/2022.

[51] The Academy of Medical Science, *Our data-driven future in healthcare*, 2018, available at: <https://acmedsci.ac.uk/file-download/74634438> (accessed August 5th 2022).

[52] High-Level Expert Group on Business-to-Government Data Sharing, *Towards a European strategy on business-to-government data sharing for the public interest,*202, available at: <https://www.euractiv.com/wp-content/uploads/sites/2/2020/02/B2GDataSharingExpertGroupReport-1.pdf > (accessed August 5th 2022).

[53] S. Castle-Clarke, *What will new technology mean for the NHS and its patients?,* 2018, available at: <https://www.nuffieldtrust.org.uk/files/2018-06/1530028974_the-nhs-at-70-what-will-new-technology-mean-for-the-nhs-and-its-patients.pdf> (accessed August 5th 2022).

[54] The Academy of Medical Science, *Our data-driven future in healthcare*, 2018, available at: <https://acmedsci.ac.uk/file-download/74634438> (accessed August 5th 2022).

between a private company and a public institute in Romania based precisely on the sharing of data and resources between these two entities has enabled patients to access innovative treatments while advancing research.[55]

3.3 Legal instruments

After analyzing the risks, solutions and undeniable benefits especially for patients, the legal instruments currently available thanks to which it may be possible for healthcare companies to access the data contained within the FSE must be evaluated. Regarding this issue it is necessary to have recourse to the provisions of the GDPR regulations, specifically the right of access by the data subject regulated by Article 15 and right to data portability regulated by Article 20.

Both articles, listed in Chapter III, rights of the data subjects, can allow patients to obtain copies of all data processed by the region in the FSE.

3.3.1 Right to access - article 15 GDPR

Article 15 of the GDPR states that *the data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data […] The controller shall provide a copy of the personal data undergoing processing […].*[56]

This right, like all data subjects' rights under the GDPR, can be exercised by all data subjects for all types of processing, including by patients for access to their health data. Since this is special data that falls within Article 9 GDPR,[57] some special arrangements need to be put in place. According to the European Data Protection Board, a data controller, before responding to the request, is required to verify the identity of the individual and ensure that the transfer is secure.

Verification of ID is an essential step before following up on the request. Precisely because of the data's sensitivity, it is necessary that before sharing the data with a person exercising the right under Article 15 GDPR, their identity must be verified with certainty by the data controller. Additionally, regarding the security, independently of the modality in which access is provided, the controller is obliged to implement appropriate technical and organizational measures to guarantee an appropriate level of security. In the event that information is provided with electronic means, the controller has to select the ones that comply with data security requirements also in regard to the transmission of the electronic file.[58]

3.3.2 Right to data portability - article 20 GDPR

According to article 20 GDPR *The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller […]. In exercising his or her*

---

[55] High-Level Expert Group on Business-to-Government Data Sharing, *Towards a European strategy on business-to-government data sharing for the public interest,* 202, available at: <https://www.euractiv.com/wp-content/uploads/sites/2/2020/02/B2GDataSharingExpertGroupReport-1.pdf > (accessed August 5th 2022).

[56] Article 15 (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[57] Article 9 General Data Protection Regulation, 2016: *Processing of 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 for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.*

[58] EDPB, Guidelines 01/2022 on data subject rights - Right of access, 2022, available at: <https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_en> (accessed: August 8th 2022).

right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.[59]

The right to data portability, introduced by the GDPR,[60] not only gives individuals the right to receive personal data, but it also allows the controller to transmit this data directly to another controller upon data subject request.[61] The limit to data portability can be deduced from the combined provisions of the recital 68 and Article 20(3) GDPR. Data portability does not apply when the data 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 data controller, or when a data controller is exercising its public duties or complying with a legal obligation.

The WP29 also within its guidelines highlighted the importance of certain necessary precautions. Such as with regard to article 15 the need to be able to identify with certainty the author of the request and put in place appropriate security measures is identified. In this specific case the WP29, already in 2017, also encouraged data controllers to develop interoperable formats that enable data portability in order to ensure easier communication and interoperability between systems.[62]

3.4 A proxy right

Thus, it seems clear that the risks can be minimized, the benefits are undeniable especially for patients, and that at least abstractly there are as many as two legal means for a private health care company to be able to obtain the sharing of data within the FSE at the request of the data subject. The Italian legal system generally allows for the possibility of a person to be represented, granting another person the power to perform legal acts and exercise rights in his own name and on his own behalf.[63]

Therefore, it is necessary to consider whether the rights under Articles 15 and 20 of the GDPR can be delegated to third parties, in particular to a company. The only limits the Italian legal system places on delegation concern the execution of very personal acts such as marriage[64] or the draft of the will.[65] Thus, from a legal point of view, in the absence of an express regulatory provision to the contrary, it is possible to consider the exercise by delegation of the rights set forth in Articles 15 ff. of the GDPR as admissible. As far as the right of access is concerned, is the Italian Data Protection Authority that admits its delegability.[66]

Although the answer on the delegability of these rights indicated within the GDPR is basically positive from a legal point of view, both rights must be evaluated individually in light of some essential elements required by delegation.

3.4.1 Delegate the right to access

---

[59] Article 20 regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[60] CNIL, *connected vehicles and personal data,* 2017, available at: <https://www.cnil.fr/sites/default/files/atoms/files/cnil_pack_vehicules_connectes_gb.pdf> (accessed: August 8th 2022).

[61] ICO website, *right to data portability*, available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/#:~:text=The%20right%20to%20data%20portability,way%2C%20without%20affecting%20its%20usability> (accessed: August 8th 2022).

[62] Article 29 Data Protection Working Party, Guidelines on the right on data portability, 2017, available at: <https://ec.europa.eu/newsroom/article29/items/611233> (accessed: August 8th 2022).

[63] Chapter VI of Title II of Book IV of the Civil Code, Art. 1387 ff.

[64] Article 111 of the Italian Civil Code.

[65] Article 601 and ff. of the Italian Civil Code.

[66] Garante della Protezione dei Dati Personali, scheda diritto di accesso, available at: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9506347> (accessed: August 8th 2022).

With regard to the right of access, it should be pointed out that from a legal point of view, the content of the proxy must present (i) the signature, including with a digital signature,[67] of the patient; (ii) present an adequately determined object; (iii) contain the express authorization for the delegate to act in the name and on behalf of the delegator; (iv) be modifiable and/or revocable at any time and (v) contain the express indication of the temporal extension and possible reiterability or not of the power of delegation.[68]

From a technical point of view, however, the mechanism of delegating access to the FSE has been implemented in a piecemeal manner by the various regions. In Lombardy it is strictly limited to those exercising parental authority or guardians, with fairly cumbersome and undigitized modalities.[69] In Emilia Romagna, delegation is also possible by electronic means by accessing one's FSE but always only to individuals.[70]

There is no standard form for drafting a proxy. Nevertheless, it is necessary that a copy of the identity document of the delegating party and the delegate be attached to the proxy. This requirement suggests a restrictive interpretation of the proxy mechanism as limited to natural persons.

At present, in Lombardy, the system is not ready by design for arbitrary delegation, so as things stand, it does not appear that any tools or processes have been prepared, to allow third parties to exercise the right of access on behalf of others.

3.4.2. Delegate the right to portability

Although the right to portability, as highlighted by the WP29, *complements the right of access,*[71] the former should be the one taken into consideration for the purpose above outlined. This is a right that would allow the state to share data between the regions that owns the processing put in place with the FSE and the private health company. Moreover, it would be possible for the latter to slice the portability request with a proxy from the patient as there are no limitations from a technical point of view.

However, there are still some obstacles related to the limits imposed by Article 20 itself that could be encountered. Those difficulties are related to the limits of applicability concerning processing based on consent or a contract excluding those necessary for the performance of a task of public interest or related to the exercise of public powers vested in the data controller. Processing carried out through FSE is not based anymore on consent[72] or a contract and may well be understood to be carried out for the performance of tasks of public interest.

3.5 IT connection with FSE (with focus on Lombardy, Italy, for "FSE1")

In Italy, with respect to the IT interaction with the FSE by the healthcare facility, it is necessary to recall Article 12 paragraph 15 bis of Decree Law n. 179/2012. In fact, it is provided

---

[67] In the case of scanning a paper document, reference should be made to Article 2712 of the Italian Civil Code: *reproductions [...] computer [...] form full proof of the facts and things represented, if the person against whom they are produced does not disavow their conformity with the same facts or things*. This means that, from a civil law point of view, only the user himself could disavow what is reported by the proxy.

[68] Article 1387 ff. Italian Civil Code; specifically articles 1392 and 1396, n form of the proxy and its modification or termination.

[69] Interrogazione a risposta scritta ai sensi dell'art.117 del regolamento generale oggetto: accesso al fascicolo sanitario elettronico, available at: <https://www.pdregionelombardia.it/pdregionelombardia/wp-content/uploads/2020/11/ITR-2876-FSE.pdf> (accessed: August 8th 2022).

[70] FSE support Emilia Romagna website, *Deleghe all'accesso FSE*, available at: <https://support.fascicolo-sanitario.it/guida/profilo/deleghe-all%26%2339%3Baccesso-fse> (accessed: August 8th 2022).

[71] Article 29 Data Protection Working Party, Guidelines on the right on data portability, 2017, available at: <https://ec.europa.eu/newsroom/article29/items/611233> (accessed: August 8th 2022).

[72] Previously art.12 paragraph 3-bis Law decree n. 179/2012 allowed treatment only on the basis of consent.

that the National Agency for Regional Health Services[73] for the enhancement of the ESF periodically adopts special guidelines that dictate technical rules related to the data coding system. It will then be up to each region to prepare a plan of compliance with them. Failure to do so will require the use of a national infrastructure or the state itself will have to exercise the region's power of substitution as provided for in the Constitution. In order to be able to enable from a technical point of view the sharing of data in Italy, it is necessary to monitor the release of the above-mentioned guidelines.[74]

Currently, the FSE infrastructure of the Lombardy Region consists of a federated information system based on the integration of the various information systems managed independently by the individual member companies. As part of the Socio-Health Information System of the Lombardy Region (SISS),[75] the platform connects central and territorial systems by enabling the management of clinical and administrative processes and access to data and services pertaining to the SISS, provided by the Socio-Health Entities and the Project Adherents. The architectural model of the SISS provides for the possibility of Application To Application (A2A)[76] integration among heterogeneous systems that allow programmatic access to the data and services in the SISS, depending on the user's authorization profile and related access permissions.

From a strictly technological point of view, therefore, there is apparently nothing to prevent a health facility from accessing data from the Lombardy FSE, once it has obtained access credentials, an authorization profile on the SISS and authorization from the patient to access the data.

4. Conclusions

Data plays a fundamental role within today's economy. It is precisely because of its importance that the need to have dedicated legislation to protect them but also to enable Europe to use the full potential of this new great wealth, including through the creation of a single market where the element of data sharing remains central to this vision. The Data Act draft, particularly with the provisions in Articles 5 and 28ff., is pushing in the right direction to allow the potential of data to be exploited to the fullest. A potential that to date is not enhanced.

As regards data sharing, too much attention is paid to the risks involved without considering possible solutions. Although they are present, as in any other treatment activity, these risks that can be mitigated by develop cybersecurity culture; adopt appropriate security measures, implement a privacy by design approach; provide the draft of the documentation required by the GDPR and create an organizational model for the sharing of responsibilities and competences in the field of privacy.

Risks should always be compared with benefits. In the healthcare sector lots of information and updated data can support medical research and innovation by allowing a medical structure to develop new health interventions. For this reason, data access across different services can improve the health care system as a whole. To benefit from it would certainly be the patients that from this policy of sharing would not only be empowered but also benefit for better care

The legal tools that currently could allow a company in the health sector to be able to access the FSE with the authorization of the patient must be sought within the GDPR. In fact, according to what is stated in Chapter III, data subjects rights, articles 15 and 20 are of interest, which regulate the right of access and the right of portability.

---

[73] AGENAS - Agenzia Nazionale per i Servizi Sanitari Regionali website, available at: <https://www.agenas.gov.it/> (accessed: August 8th 2022).

[74] Art. 12 co. 15 *bis* Decreto Legge n. 179/2012 es modified by Decreto Legge n. 4/2022.

[75] Sistema Informativo Socio Sanitario SISS web site available at: <https://www.siss.regione.lombardia.it/wps/portal/site/siss> (accessed: August 8th 2022).

[76] Regione Lombardia website, *Integrazione Application to Application (A2A),* available at: <https://www.siss.regione.lombardia.it/wps/portal/site/siss/il-sistema-informativo-socio-sanitario/piattaforma-siss/integrazione-application-to-application> (accessed: August 8th 2022).

The Italian legal system generally allows for the possibility of a person to be represented, granting another person the power to perform legal acts and exercise rights in his own name and on his own behalf. Although the answer is basically positive from a legal point of view on the delegability of these rights indicated within the GDPR. If deeply analyzed this possibility for both rights turns out: it is impossible as regards the right to access, and very complex for the right of portability.

Instead, from a strictly technological point of view, as above demonstrated, there is apparently nothing to prevent a health facility from accessing data from the Lombardy FSE, once it has obtained access credentials, an authorization profile on the SISS and authorization from the patient to access the data.

After all the above mentioned it is clear how opportunities for the sharing and re-use of data combined with the removal of technical and legislative barriers provided by new and updated legislation can have a great positive impact not only for the healthcare sector but also for patients. If the Data Act proposal is approved it would allow under Article 5 a private health care company to be able to have access to the FSE of its patients upon their authorization. This would overcome the limitations found and reported on, in the use of data subjects' rights provided for in Articles 15 and 20 of the GDPR. Furthermore, even if in the specific case considered, as reported, there are no issues from a technical point of view, the provision of Article 28 of the Data Act in relation to interoperability would enable and facilitate the exchange of data.