

EURORDIS POSITION ON THE EUROPEAN HEALTH DATA SPACE

(please note: design of the document will be changed after the review process. Table of contents, summary, reference list etc will be added at the final stage).

Introduction

On 3rd May 2022, the European Commission launched the proposal for a Regulation for the European Health Data Space (EHDS)¹. Once adopted, the legal act could become a fundamental game changer for digital transformation of health sector in the EU. The draft proposal aims to (1) give individuals increased digital access to and control over their personal health data; (2) define common mandatory standards for electronic medical record systems to ensure their security and interoperability; (3) create consistent framework for secondary data health data uses for the needs of research, innovation, policy-making, patient safety and other regulatory activities.

There are 6000 various rare diseases affecting over 36 million people across Europe.² However, only 6% of all known rare diseases have curative treatment. The rare disease community has many unmet needs. The limited number of patients alongside the scarcity of available knowledge and expertise on these diseases, make rare diseases a field that could greatly benefit from the European action. Thus, the EHDS offers new opportunities to ultimately improve the lives of people living with a rare disease through enhanced and safe access to data to advance diagnosis, treatment, care and research for rare disease patients.

The following position paper provides recommendations and views of the rare disease community on the primary health data uses, secondary health data uses, digital health literacy and patient/public partnership.

I. EUROPEAN ELECTRONIC HEALTH RECORD EXCHANGE FORMAT – PRIMARY HEALTH DATA USES

Electronic Health Record (EHR) systems are an essential tool to support healthcare, as they facilitate primary health data uses - processing personal electronic health data for the provision of health services to assess, maintain and care for the state of health of a person to whom data relates. EHR systems are also highly relevant for doctors, as they allow to easily share health information with different specialists. Thus, is often the case in the context of cross-border healthcare services for rare disease patients, as rare disease patients often have to consult specialists in different countries.

For patients to fully benefit from the creation of the European electronic health record exchange format, we call on to ensure:

- **Implementation and the use of ICD-11 and ORPHA codes in EHR systems**

Because of their individual rarity, genetic diseases and other types of rare diseases are under-represented in healthcare coding systems. This contributes to lack of recognition of their importance and hinders collection of high-quality data needed for healthcare and research purposes.³ Absence of a comprehensive coding system also results in a delayed diagnosis, treatment and care setbacks. The International Classification of Diseases (ICD) has long been the main basis for comparability of statistics on causes of mortality and morbidity between places and over time. In 2019 the World Health Assembly adopted a revised version – ICD-11, which is significantly more expressive and comprehensive than historical versions, and which also includes rare diseases. To enhance data collection and its quality for healthcare purposes and beyond, it is of key importance to make ICD-11

¹ https://health.ec.europa.eu/publications/proposal-regulation-european-health-data-space_en

² https://health.ec.europa.eu/non-communicable-diseases/steering-group/rare-diseases_en

³ <https://ojrd.biomedcentral.com/articles/10.1186/s13023-015-0251-8>

use mandatory within the EHR systems across the EU, as well as other databases collecting data about rare diseases. Furthermore, implementation of ICD-11 has to go hand in hand with trainings and other capacity building activities to make sure those involved do have necessary knowledge to use the classification.

- **Secure EHR systems through adoption of high data processing, encryption and storage standards, in line with the GDPR, NIS2 and other relevant laws;**

Data protection is a fundamental condition to ensure citizens' trust in EHRs systems. Establishing universal and binding standards for the security of the data stored in the EHRs systems should be guaranteed by the Regulation. Furthermore, it is not only about making such standards part of the law but also making necessary investments and ensuring a consistent oversight and enforcement and necessary elements for make a real change.

- **Making publicly certified eIDs through Electronic Identification, Authentication and trust Services (eIDAS⁴) the preferred method of identifying individuals when they use EHR systems and other health information systems**

eID is a set of services provided by the European Commission to enable the mutual recognition of national electronic identification schemes (eID) across borders. It allows European citizens to use their national eIDs when accessing online services from other European countries. To strengthen and enhanced data protection, publicly certified eIDs should become a legally mandatory method to connect to the EHR and other health information systems, as opposed to some private initiatives (e.g. Facebook or Gmail login) to enhance both user and system protection.

- **EHR systems and data protection policies must be developed in line with the following rights:**

Right to an immediate access to personal electronic health records

&

Right to have a copy of the personal electronic health records

Providing individuals with an easy access to their health information empowers them to be more in control of decisions regarding their health and well-being.⁵ Access to personal health records, and easily obtainable copy of information could facilitate condition monitoring, adherence to treatment plans, tracking progress and it could significantly contribute to saving costs and speeding up diagnosis process, as individuals would not need to repeat unnecessary tests when moving from one healthcare specialist/provider to another. This is especially relevant for rare disease patients who often seek healthcare services from multiple specialists.⁶

Right to data portability

Right to portability enables individual to move certain personal data they have provided from one platform to another offering similar services. It is essential to allow individuals to decide what happens to the data they generate, when they share it and with whom. It should be a simple process to allow individuals to easily move their health data across different services in a safe way. To

⁴ https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

⁵ <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html>

⁶ <https://journals.sagepub.com/doi/full/10.1177/1473779520914290>

	<p>date, this right has been largely neglected in healthcare due to the low interoperability of the EHR systems.</p>
<p>Right to allow or restrict personal electronic health data sharing with a selected healthcare professional</p>	<p>Individuals should be able to restrict access to certain parts of their records. E.g., when an individual visits a dentist, they should be able to e.g. restrict access to information about their abortion. However, such right should be exercised/granted only in situations when restricting access to information would not put in risk individual's health and well-being.</p> <p>Individuals should be informed every time a healthcare professional who is not directly treating them requests access to their health records and should be asked to give the authorisation to access to the whole file, or parts of the file, or no access at all before the information is accessed.</p>
<p>Right to data rectification</p>	<p>Individuals should have right to request data rectification and correct possible errors, misdiagnosis or other inconsistencies in their medical records or medicine prescriptions. This should only be done with the approval from the healthcare professional.</p>
<p>Right to have information about who and when accessed patients' personal electronic health record</p>	<p>It should be visible in the system of the EHR who and when has accessed EHR and its parts, to minimize the risks of unauthorised access.</p>
<p>Right to be forgotten</p>	<p>Right to be forgotten, also known as the right to erasure, is one's right to request a data controller to delete their personal data.</p> <p>However, based on the General Data Protection Regulation (GDPR), it is not an absolute right, as it can only be exercised under specific circumstances (see GDPR Article 17⁷). In addition, to these conditions, an organisation's right to process someone's data might overrule individual right to be forgotten. E.g. the data is being processed for public health purposes, when the data is necessary to perform preventative or occupational medicine or the data what represents important public or scientific research interest. Even though conditions to application of this right apply, it is important to consider each individual case, and where possible, fulfil the request of an individual.</p>
<p>Right to file a complaint to the National (Health) Data Protection Authority</p>	<p>Individuals should be sufficiently informed about their GDPR-granted right to file a complaint to the National (Health) Data Protection Authority.</p>

⁷ <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

II. RESEARCH, POLICY-MAKING - SECONDARY HEALTH DATA USES

The rarity of diseases means information and data about them is scarce, as there are often too few people in a geographic location to gather necessary knowledge. Poor understanding of the pathophysiology of rare diseases remains a significant one, and this is not only a challenge when formulating treatments to combat the disease: it also results in under- or misdiagnosis, endangers patient health and causes downstream issues for clinical trial patient selection. Data is vital to progress knowledge on rare diseases and address this important public health concern.

However, it is crucial that increased data sharing for research, innovation, policy-making, patient safety and other regulatory activities does not come at the price of patient rights. With the EHDS creation, it is likely that health and research data sharing will increase greatly. While increased access to large volumes of sensitive data could significantly improve knowledge on rare disease, it also makes the individuals more vulnerable. The nature of risk is no longer limited to the risk of physical or psychological harm, but also includes the risk of informational harm, such as privacy breaches, algorithmic discrimination, profiling.⁸ In the context of genetic information the risk is not only restricted to the individual but to their family and generations to come.

In the instances, where health data comprises personal data, the Member States have quite diverse approaches when it comes to legal bases for data processing (based on the GDPR exemptions). In some Member States data subjects are mandated to provide consent for research or other secondary purposes, while in others it is encouraged to rely on alternative bases for processing (without consent but with other safeguards). While it preserves uniqueness of national healthcare systems, it is negatively impacting cross-country research, as there is a lot of confusions and delays due to unharmonized rules. The EHDS proposal aims to facilitate a more coherent approach to health data secondary uses by establishing bases for processing, safeguards for processing and governance mechanisms for providing access to health data. While establishing a much welcomed consistency and achieving the right balance between research /other needs and an individual risks, it is important to consider the following:

- **Establishing data governance models for individuals to exercise control over their re-purposed data**

Data governance refers to the exercise of authority and control over the management of data.⁹ Informed consent and medical confidentiality have traditionally been used as mechanisms of data control in the health sector. However, in today's data-intense environment they seem to offer only limited amount of control over the production, collection, use, and circulation of health data. Consent procedures often fall short of adequately informing data subjects about the terms of use of their data, and in the context of data patients may experience a substantial lack of control over the flow of their data. Furthermore, traditional mechanisms such as informed consent are of limited value when it comes to the evaluation of big data research due to the quantity of data. For instance, it may not be realistic to obtain an informed consent on a retrospective study involving millions of individuals.

Thus, in addition to exploring novel consent models such as dynamic consent, there is a need to create participatory health data governance schemes within the EHDS to ensure secure, ethical data access and safe environment while providing clarity and means to control health data uses to patients. It is important to note, that the introduction of new elements for data control does not exclude the use of

⁸ <https://bmcmethics.biomedcentral.com/articles/10.1186/s12910-021-00616-4>

⁹ <https://www.sciencedirect.com/science/article/abs/pii/S0268401219300787>

the ‘traditional’ methods: depending on the situation, setting, individual preferences different models should be explored.

Establishing public engagement (multi-directional communication, consultation, and participation) into health data governance is needed to ensure transparency of the EHDS, promote accountability and foster the trust, and it is a necessary ethical condition. It is also necessary to formally involve patients into the governance structure to ensure that individual data is used with respect and in the best public interest, given a proposed rule that health data access bodies shall not be obliged to provide specific information to each natural person concerning the use of their data for projects and shall provide only general public information.

However, health data comes from many sources, takes different formats, stored in multiple systems and requires a variety of accessibility procedures, includes diverse uses and users. What is more, health data concepts are complex, involve technical language, medical and legal jargon. Therefore, there may not be one model what fits all when it comes to health data governance and meaningful patient engagement. See Part IV of the paper for the proposed model.

What is dynamic consent?

Dynamic consent is a personalised, participant-centred communication interface to enable research participants to be in the centre of the decision-making on what happens with their data. This approach is ‘dynamic’ as it allows interactions over time, allowing participants to consent to new projects, withdraw their consent or make other choices in real time as their circumstances change. Dynamic consent model does not restrict participants to the opportunity to give broad consent only but allows them to provide different types of consent depending on the kind of study. These consent preferences travel securely with their samples or data so that third parties know the scope of the consent that applies. Dynamic consent goes beyond informed consent and could help individuals to control their data and online presence. For the dynamic consent model to be successfully implemented it should be specified when consent decisions are required, when decisions should be reviewed, which data are held and stored, where and how the consent decisions are connected with data.¹⁰

- **European Reference Networks (ERNs) to assess the feasibility of the EDHS to enable data uses for secondary purposes**

It is crucial to assess how the new obligations and models will be implemented in practice, as well as setting realistic timelines to comply with these new obligations. ERNs could serve as a testing hub to assess the feasibility, time and resources needed for data holders to enable secondary uses and comply with the obligations to respond to single data requests. The results of this could inform the legislative process itself, help to establish reasonable transition periods, and to inform the future implementing and delegated acts.

- **Ensuring strong standards for data anonymisation, pseudonymisation and additional safeguards for both personal and non-personal sensitive data categories**

Anonymisation makes a data set non-identifiable by removing personal identifiers (full anonymisation) or by replacing them with keys that the original data controller can use to re-identify the data (pseudonymisation).¹¹ Anonymised data is considered non-personal data and falls out of the GDPR’s scope, while pseudonymised data is considered personal data and are subject of the GDPR regime.

¹⁰ <https://www.nature.com/articles/ejhg201471>

¹¹ https://edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf

While both techniques are considered as data privacy enhancing mechanisms, anonymisation technologies do not guarantee full privacy, since increasing capabilities in data analytics make the data re-identifiable. Therefore, absence of clear standards for strong anonymisation may contribute to creating a false sense of security and ultimately a false sense of control. Furthermore, mixed datasets including both personal and non-personal data may increase the risk of re-identification and full data anonymisation does not enable individual control over the data use for specific purposes, whereas some of such purposes may not be desirable to an individual due to ethical reasons. For these reasons there is a need to put additional safeguards and data control mechanisms for anonymised and pseudonymised health data. The following elements might be considered:

- Data stewardship, specifying the roles and responsibilities around data management and accountability.
- Data policies and procedures to manage data sets, including enforcing authentication and access rights to data as well as the organisational measures and policies to ensure the quality, accuracy and security of the data and regulatory compliance. Tools to help preserve the autonomy and rights of individuals to control their data.
- Data standards, specifications and rules for the definition, creation, storage and usage of data.¹²

- **Defining the clear role for the Research Ethics Committees (RECs) in big data health research**

As traditional approaches of health research are being challenged in the context of big data, there is a need to also redefine the role of the Research Ethics Committees (RECs). The main function of RECs is to protect research participants by identifying ethical issues posed by research involving human subjects.¹³ However, the mandate of RECs is not clear when it comes to assessing the risks and benefits of research projects involving big data and analytics, and some areas of the big data research remain unregulated. For instance, it is up to each EU Member State to define whether research based on anonymised data should seek ethical review.¹⁴ Whereas, traditionally anonymised data is considered to be lower risk for an individual, as such concept of harm has only been linked to vulnerability in data protection. However, the risks of anonymised/aggregated big data are not only limited to an individual privacy, but such risks also involve group discrimination (e.g., anonymised data reveal health patterns of a certain sub-group) or dignitary harm¹⁵. In addition, as mentioned previously, anonymised data does not offer a bulletproof guarantee from re-identification. Especially when it comes to rare disease data, which due to its scarcity may not even be anonymised. Given the complexities of technological advancements, as well as emergence of new risks and harms linked with big data health research, there is a need to clearly define the mandate of RECs and develop a common methodology to assess big data projects both in case of personal and non-personal data uses.

- **Making rare disease patient data FAIR**

Rare disease patient data are typically sensitive, present in multiple registries controlled by different data controllers, and non-interoperable. Making these data Findable, Accessible, Interoperable, and Reusable (FAIR) for humans and machines at source enables federated discovery and analysis across

¹² No time to lose: Building a data strategy for the European Reference Networks, EURORDIS, April 2020

¹³ <https://journals.sagepub.com/doi/pdf/10.1177/174701610700300110>

¹⁴ <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8085804/>

¹⁵ Article 7 of the Charter of Fundamental Rights of the European Union protects the dignity of persons by regulating inappropriate communications that threaten to degrade, humiliate, or mortify them. Dignitary privacy follows a normative logic designed to prevent harm to personality caused by the violation of civility rules.

data controllers, processors and holders. This facilitates accurate diagnosis, optimal clinical management, and personalised treatments.

- **Ensuring public return on data investment**

Given a high value of health data which would be increasingly shared by the individuals, it is important not to reduce the data to a commodity that do not bring a societal benefit. While direct payments to the individuals raise a number of ethical concerns and may lead to unfair practices, it is also problematic not to have any 'return' of investment on the commercialised gains of data. One of the options to guarantee such return would be to 'pay back' to the society, instead of an individual gain. For instance, if thanks to data made available through the EHDS for research, a medicine or treatment are developed and are used commercially, conditionalities should apply. A conditionality may include a requirement to allow research results use to other parties and not 'lock in' the acquired knowledge within one entity, independently if research led to a desired outcome or not. There could also be a conditionality to make medicines developed thanks to use of public data affordable, thus acknowledging a societal contribution of data as a valuable input into the research outcome.

III. DIGITAL HEALTH LITERACY

Digital health literacy is a critical component for individuals, healthcare professionals, researchers and other involved stakeholders to have necessary skills to be able to meaningfully participate in a newly created system, as well as fully benefit from it. Digital health literacy can be considered as convergence of both digital literacy and health literacy. However, certain competences of digital health literacy may not be covered by neither digital literacy nor health literacy, therefore it is important to make a distinction.¹⁶ The Transactional Model of Digital Health literacy outlines for competence levels of digital health literacy¹⁷:

- (1) *Functional*: the ability to successfully read and write about health using technological devices;
- (2) *Communicative*: the ability to control, adapt and collaborate in communication about health with others in online social environments.
- (3) *Critical*: the ability to evaluate the relevance, trustworthiness, and risks of sharing and receiving health-related information through the digital ecosystem;
- (4) *Translational*: the ability to apply health-related information from the digital ecosystem in different contexts.

It is necessary to include these elements into educational programmes targeting specific groups. Development of the EHDS must go hand in hand with digital education of healthcare professionals and patient communities to ensure a successful and patient-centered implementation of the EHDS. The proposal should put in place mechanisms to ensure educational and capacity building assistance to patients to better understand their rights and obligations on how to manage their health data, when it comes to uses of both primary and secondary health data. It is a crucial component to ensure a well-functioning data sharing infrastructure at the EU level, without sufficient digital literacy levels of end users, the system put in place will not be properly used. Rare disease community might need specifically designed educational programmes due to the unique link with the ERNs and frequent uses of highly sensitive data categories such as genetic data. A supportive profession specialised in healthcare digitalisation should be present to provide expertise to both healthcare professionals and patients where needed.

In addition, given a unique placement of patient organisations and civil society organisations, they can play a trusted offline role to coordinate data sharing and management, enable informed choices for

¹⁶ <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8861384/>

¹⁷ Journal of Medical Internet Research - Proposing a Transactional Model of eHealth Literacy: Concept Analysis (jmir.org)

patients to share or not their health-related data and supporting the implementation of the European Health Data Space. Moreover, patient and civil society representatives can play a significant role in the development of new tools to control data use through the participatory arrangement of data models - e.g. acting as data cooperatives¹⁸.

IV. PATIENTS and PUBLIC PARTNERSHIP

Patient partnership is a mutual relationship between persons living with a rare disease and other stakeholders where input from people living with a rare disease or caring for someone with a rare disease routinely and formally informs policy reflections and decisions. Patient partnership implies going beyond empowerment and engagement but considering people living with a rare disease and their advocates as equal partners and actors in policy and programme design and evaluation.¹⁹

Patient partnership within the EHDS system could significantly increase public understanding of the created health data space, help them to navigate through the complex issues, allow individuals to ensure that their data is used with respect to the set rules and in the best public interest. What is more, it would ensure a better understanding of data sharing pros and cons, weigh them and manage expectations accordingly.

The EHDS will establish several governance structures at national level, such as health data access bodies, digital health authorities, and European level - European Health Data Space Board. We call on to involve patients and civil society representatives into each structure, potential partnerships models could be explored:

- **National Public Advisory Board for Health Data embedded in the Health Data Access bodies' governance structure**

Composed of individuals or carers of people whose data is made available by the Health Data Access Body with a goal to consult and provide feedback to the Health Data Access Boards on individual-centered data sharing. Some of its members could be actively involved in Health Data Access Bodies decision making groups (e.g. Access Review Committee, Ethics Advisory Committee).

- **Digital Health Citizen Panel**

Citizen Panels composed of citizens randomly selected could serve as an Advisory body to the national Digital Health Authorities to provide feedback on diverse matters linked with national healthcare system digitalisation. Sampling methodologies would need to ensure that the panels are representative of each country local communities in terms of geographic origin, gender, age, socioeconomic background and level of education.

- **European Societal Advisory Board**

European Societal Advisory Board embedded in the EHDS Board governance structure, composed of 27 national citizen representatives could play an advisory role to the European Health Data Space Board. Sub-groups may be created to work different topics – e.g. a Chair that is a member of the EHDS Board executive board and reports directly to the EHDS Executive Board, and some other members who would be actively involved in the EHDS Board working groups.

¹⁸ A health data cooperative is a collective where health related data are integrated, stored, used, and shared under the control of the cooperative members.

¹⁹ <https://www.rare2030.eu/>

Key functions of patient/civil society consultative bodies



Oversee data access process



Protect participants' interests in research and decision-making



Share experiences and advice



Listen and respond to societal feedback on the EHDS elements