Technology and Regulation

The Impossible Job of Health Data Access Bodies under the European Health Data Space – A technocratic colossus or rubber stamp forum?

Author(s)	Paul Quinn
Contact	paul.quinn@vub.be
Affiliation(s)	Paul Quinn is a Law Professor at the Vrije Universiteit Brussel (VUB – Free University of Brussels)

Keywords	European Health Data Space, GDPR, Health Data Access Body, scientific research, secondary data
Published	**Received**: 6 nov 2024 **Accepted**: 25 feb 2025 **Published**: 22 May 2025
Citation	Paul Quinn, The Impossible Job of Health Data Access Bodies under the European Health Data Space – A technocratic colossus or rubber stamp forum?, Technology and Regulation, 2025, 60-80 • 10.71265/vbfvpb76 • ISSN: 2666-139X

Abstract

The legislative text for the European Health Data Space (EHDS) has sparked extensive discourse, weighing the potential benefits for healthcare and innovation against concerns over privacy and societal impacts. At the heart of this discussion is the role of the Health Data Access Body (HDABs). These entities will be tasked with managing the reuse of secondary health data within the EHDS framework. This article delves into the formidable challenges facing HDABs, suggesting that the complexity and volume of data access requests may overwhelm their capacity. Ensuring compliance with EHDS regulations, GDPR provisions, and ethical standards presents a multifaceted challenge. This paper argues that the expertise and efficiency required to navigate these complexities could strain HDAB resources and capabilities. Furthermore, the anticipated surge in data access requests may exacerbate these challenges, potentially compromising HDAB effectiveness. Consequently, there is a pressing need for a pragmatic approach to delineating HDAB responsibilities to ensure their ability to fulfill their role competently. By addressing these concerns, the EHDS can uphold individual rights, promote societal welfare, and foster trust in its overarching objectives.

1. Introduction

The concept of a European Health Data Space (EHDS) has stimulated much debate.[1] This debate relates not only to the potential benefits it may offer to healthcare, research and innovation but also potential harms to individual privacy and societal interests. Health Data Access Bodies (HDABs) will have a central role to play in the proposed EHDS. The EHDS regulation leaves it open to Member States to decide what forms HDABs will take in their jurisdiction, how many there will be, and what their specific competences shall be.[2]

They *will inter alia* co-ordinate the reuse of secondary data that will be made available by data holders.[3] In doing so they will have a crucial role to play in ensuring that electronic health data is made available for reuse by appropriate entities, under appropriate conditions and for valid reasons. As this article will discuss, doing so will entail a range of highly complicated and resource demanding tasks. This article will explore the difficult and complex mission that this entails. In doing so the author of this paper will argue that the complexity of these tasks, together with the potentially high volume of data access requests and the requirement that requests should be dealt with relatively quickly means that HDABs have been given a potentially impossible task, raising the risk that some may become overburdened and unable to carry out their work in a way that appears to be envisaged in the regulation.

This analysis in this article involves three main steps. The *first* will analyse the requirements that the EHDS regulation places upon HDABs when determining whether of not to grant a data access permit.The *second* step is to look at what these requirements are likely to mean in the many and varied contexts (given both the variation in national law and potential heterogeneity in the nature of Electronic Health Data) the EHDS is likely to operate within). The third will look the need of HDABs to take into account these requirements and contexts in an environment where they may have to respond to a potentially high volume of requests in a limited time frame.

Section 2 of this article will outline the background of the EHDS and its main *raisons d'être*, one of which is to ensure access to secondary electronic health data for a range of purposes through the granting of Health Data Access Permits. Section 3 will outline the mandate that HDABs are given under the EHDS regulation. It will also outline some of the uncertainties that remain over the form they will take and their likely variation from country to country.The remainder of the paper will then focus on some of the key determinations that HDABs must make when deciding whether access permits should be granted or not. This includes ensuring that Articles 53 and 54 (outlining broad reasons for when electronic health data can and cannot be shared) of the EHDS regulation are complied with (section 4), that the data recipient has a valid legal base under the GDPR and that key data protection principles such as minimization and storage limitation are likely to be respected (section 5) and that relevant rules on ethical review at the national level have been complied with (section 6). These areas do not represent all the responsibilities upon HDABs under the EHDS but have been identified as the main factors that these bodies must take into account when deciding (or not) to grant health data access permits.[4]

As the author will discuss in section 7 these demands will likely require a considerable intensity and speed of review that HDABs will find it difficult to meet unless they are very well resourced. This is due to the wide

1. This paper is based on the final and published version of the EHDS regulation i.e. "Regulation of the European Parliament and of the Council on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 - 2022/0140(COD)". Available at https://data.consilium.europa.eu/doc/document/PE-76-2024-INIT/en/pdf
2. The "Health Data Access Bodies – Community of Practice" has been established to aid Member States in the creation of HDABs in the first years of the EHDS. It aims to develop collaboration facilitating the establishment of HDABs and to share best practice once it is established. For more go to: https://health.ec.europa.eu/ehealth-digital-health-and-care/eu-cooperation/health-data-access-bodies-community-practice_en
3. As the explanatory notes to the original EHDS proposal state on page 1 "It also aims to ensure a legal framework consisting of trusted EU and Member State governance mechanisms and a secure processing environment. This would allow researchers, innovators, policymakers and regulators at EU and Member State level to access relevant electronic health data to promote better diagnosis, treatment and well-being of natural persons, and lead to better and well- informed policies." For more see: the first proposal draft 'COM(2022) 197 final 2022/0140 (COD)'.
4. These responsibilities of HDABs when deciding upon data access permits are outlined in article 67 of the regulation.

range of competences that are likely to be required in reviewing requests, ranging from legal and ethical expertise, in addition to being able to firmly grasp the scientific or technical background of a particular dossier. In addition, the potentially large number of requests that HDABS's are likely to receive, particularly in larger Member States, may translate to a very heavy work load. This results in the risk that they will not be able to perform their function adequality with attendant risks for individuals, society and overall trust in the concept of the EHDS. Given this the author of the paper opines that it would be prudent to conceive of the tasks given HDABS in a more pragmatic way in order to ensure they are executed in a competent manner.

2. The Main Goals of the European Health Data Space

The EHDS is a complex, multi-faceted initiative that has diverse goals. Perhaps the two most prominent of these goals are to improve health data sharing within primary care and to make electronic data more readily available for a range for secondary processing for a range of purposes.[5]

In terms of the former the EHDS aims primarily to facilitate improved sharing of electronic health records (EHRs) or elements from them between healthcare providers based not only within the same Member State but also between those in different Member States. It will do this by *inter alia* requiring that all EHRs adopt the same standards[6] and by requiring Member States to facilitate the transfer of EHR data (or priority elements therein) between different healthcare providers in different Member States.[7] The goal behind doing so is to allow individuals to access healthcare either remotely or physically in other Member States with greater ease.[8]

In terms of the latter (i.e. the area this paper is primarily concerned with) a primary aim of the EHDS framework is to improve access to electronic health data for a range of secondary processing processes.[9] These can vary from classic forms of scientific research, to aiding public bodies in the health or social sector to performing their mandates, to aiding innovation in the private sector.[10] In order to facilitate this the EU Commission aims to establish entities known as 'Health Data Access Bodies' (EDABs) in all Member States. These bodies will be given several important tasks relating to the re-use of secondary electronic health data. These include being informed of secondary data that is held by relevant 'health data holders' and inventorying it.[11] This will allow potentially interested data recipients to submit a data access request

5. The duality of the regulation in terms of its two main aims is clearly outlined in recital 1 of the proposal which states: "The aim of this Regulation is to establish the European Health Data Space ('EHDS') in order to improve access to and control by natural persons over their personal electronic health data in the context of healthcare, as well as for other purposes that would benefit the society such as research, innovation, policy-making, patient safety, personalised medicine, official statistics or regulatory activities."
6. Article 15 of the EHDS regulation provides a framework for the creation of a 'European electronic health record exchange format". The precise details shall be laid down by future EU Commission Implementing acts.
7. Article 14 of the EHDS regulation.
8. This aspect and its links to the GDPR right of data portability has been discussed by the author in a recent paper: Wenkai Li and Paul Quinn, 'The European Health Data Space: An Expanded Right to Data Portability?', *Computer Law & Security Review*, 52 (2024), 105913 https://doi.org/10.1016/j.clsr.2023.105913.
9. The provisions relevant to this are outlined in Chapter IV of theregulation.
10. As section 4 of this paper will further outline Articles 53 and 54 of the EHDS regulation specify a range of contexts for which a data access permit should and should not be granted.
11. The defintion of 'health data holder' was refined and expanded in the final consolidated version of the EHDS, elaborated in article article 2(2)(y) as "health data holder' means any natural or legal person, public authority, agency or other body in the healthcare or the care sectors; including reimbursement services when needed as well as any natural or legal person developing products or services intended for the health, healthcare or care sectors; developing or manufacturing wellness applications; performing research in relation to the healthcare or care sectors; or acting as a mortality registry; as well as any Union institution, body, office or agency; who has either: (i) the right or obligation, in accordance with applicable Union or national law and in its capacity as a controller or joint controller, to process personal electronic health data for the provision of healthcare or care or for the purposes of public health, reimbursement, research, innovation, policy making, official statistics or patient safety or for regulatory purposes; or (ii) the ability to make available non-personal electronic health data through the control of the technical design of a product and related services, including by registering, providing, restricting access to or exchanging such data".

to HDABs to receive electronic health data for secondary processing.[12] Upon reception of such a request HDABs will have to analyse it to see if it meets a number of requirements outlined within the EHDS. Once it has determined that the correct conditions are in place the role of the HDABs is to grant such a permit and to facilitate access to the electronic health data in question in a suitable manner.[13] If such a permit is granted, HDABs should notify applicants with their decision specifying the general conditions applicable to the data, the types and format of electronic health data to be covered by the data permit (including their sources), the purposes for which such data can be processed and for how long the data permit is valid. They should also describe how such data may be processed in a 'secure processing environment'[14] controlled by the HDAB.

The remainder of this article will focus on the difficulties HDABS are likely to have in deciding upon the validity of data access requests and what conditions should be attached to them. As indicated in the introduction to this article, this will be done in three ways. The *first* relates to the requirements that the EHDS regulation places upon HDABs when determining whether of not to grant a data access permit.The *second* relates to what these requirements are likely to mean in the many and varied contexts (given both the variation in national law and potential heterogeneity in Electronic Health Data) the EHDS is likely to operate within. The *third* concerns the need of HDABs to consider these requirements and contexts in an environment where they may have to respond to a potentially high volume of requestions in a limited time frame. As section 7 will discuss in further detail, these challenges will call into question the feasibility of the very role that HDABs have been given.

3. The Mandate of Health Data Access Bodies

Each Member state must create an HDAB, and they should be sufficiently resourced to carry out their functions effectively.[15] In addition to deciding upon the validity of data access requests, they have a number of technical roles to play in the facilitation of electronic health data sharing for subsequent secondary processing. These include *inter alia* cataloging available electronic health data and creating the conditions for it to be processed in a safe way (i.e. where possible ensuring anonymization or a 'safe processing environment').[16]

In terms of the decision to grant a data access permit, HDABs may only grant data access when a number of key criteria are met. Some of these stand out because they will seemingly require significant enquiries and analyses on the part of HDABs. The *first* is that the proposed processing purpose be in line with the criteria outlined in articles 54 and 54 of the EHDS regulation. Article 53 provides a list of contexts for which a data access request should be granted. Conversely Article 54 provides a list of contexts for which a data access request should not be granted. As the Regulation states in Article 68, before granting a health data access permit HDABs must assess:

12. The relevant provisions specifying the requirements of data access permit requests and the permits themselves are found within Chapter IV Section 3 of the regulation. Article 67 outline how a data access application must be made.
13. Article 68 of the regulation outlines the procedure HDABs should use for issuing a permit.
14. The concept of a secure processing environment relates to a processing environment established by the HDAB that reduces privacy risks for potential data subjects. This could include for example a federated processing environment that does not allow external parties to remove personal data (though they may be able to process it within the confines of the secure processing environment. Further potential measures are outlined in article 73 of the EHDS proposal. For more on secure processing environments see: E. Soini, T. Hallinen, and J. Martikainen, 'RWD31 Secure Processing Environments (SPE) Are Needed for the Cybersecure Collection and Secondary Use of Personal, Health, and Social Data', *Value in Health*, 25.12 (2022), S453–54 https://doi.org/10.1016/j.jval.2022.09.2256.
15. Article 55 of the EHDS regulation
16. Article 57)(1)(b) of the EHDS regulation states HDAB's are responsible for"processing electronic health data referred to in Article 51 such as by receiving, combining, preparing and compiling such data when requested from health data holders and the pseudonymisation or anonymisation of those data ..." Article 57(1)(a) states that HDABs are responsible for "deciding on health data access applications pursuant to Article 67 of this Regulation, authorising and issuing data permits pursuant to Article 68 of this Regulation to access electronic health data falling within their remit for secondary use and deciding on health data requests submitted pursuant to Article 69 of this Regulation"

- the purpose described in the data access application matches one or more of the purposes listed in Article 53(1) of this Regulation;
- the requested data is necessary, adequate and proportionate for the purpose or purposes described in the health data access application taking into account the provisions of data minimisation and purpose limitation in Article 66;
- the processing complies with Article 6(1) Regulation (EU) 2016/679, in particular that in the case of pseudonymized data, there is sufficient justification that the purpose cannot be achieved with anonymized data;
- the applicant is qualified *vis-à-vis* the intended purposes of data use and has appropriate expertise, including professional qualifications in the areas of healthcare, care, public health, research, consistent with ethical practice and applicable laws and regulations;
- the applicant demonstrates sufficient technical and organisational measures to prevent misuse of the electronic health data and to protect the rights and interests of the data holder and of the natural persons concerned;
- the information on the assessment of ethical aspects of the processing, where applicable, is in line with national law.

Importantly, these conditions are cumulative. This means for instance that even where a proposal for access to electronic health data is seemingly in line with articles 53 and 54 of the EHDS regulation a HDAB should not grant access to the data in question where such processing would contravene the GDPR. The EHDS therefore can be thought of incorporating multiple levels of protection against potential misuse. In addition, the EHDS legislation will not create *lex specialis* data protection law, with the exception of the elements of the regulation that give rise to a legal basis for HDABs themselves to process electronic health data under the EHDS. This means that the applicable provisions of the GDPR will apply to those wishing to process health data under the EHDS.This may have been deemed necessary to ensure a high level of protection and trust in an area that involves using data that is considered extremely sensitive both from an individual and societal perspective.[17] The details of these protective elements and the challenges they bring with them for HDABs are discussed in the sections that follow below.

4. Complying with Articles 53 and 54 of the EHDS Proposal

Article 53 presents a list of contexts for which a data access permit can be approved. Conversely article 54 presents a list of contexts for which a data access permit should not be approved. It is the task of HDABs to determine whether one of these contexts applies and act accordingly. Together, these two articles outline numerous contexts, some of them being notably broad in nature and, as a consequence, difficult to define concisely.[18] The result is that there is a large room for discretion given to HDABs to determine whether the conditions in question have been met. As the author has discussed in a sperate paper, the sheer discretion given to HDABS in articles 53 and 54 is itself an important concern of the proposed EHDS framework that is deserving of further consideration.Exercising the considerable discretion bestowed upon HDABs by these articles will (as the subsections below further outline) require both a considerable effort in terms of policymaking on the part of HDABs and also detailed reflection of the facts of each request for a data access permit. This will arguably represent a significant workload for HDABs.

4.1 Reasons to grant a data access request (article 53)

The EHDS regulation foresees numerous contexts for which it may be acceptable to make electronic health data available for secondary processing. Whilst going through these grounds systematically is beyond the

17. These protections have not been sufficient to allay the concerns of a number of commentators. This includes a group that argues that the EHDS should be based primarily on a form of standardized consent. See for example: Stefanie Brückner and others, 'The Social Contract for Health and Wellness Data Sharing Needs a Trusted Standardized Consent', *Mayo Clinic Proceedings: Digital Health*, 1.4 (2023), 527–33 https://doi.org/10.1016/j.mcpdig.2023.07.008.

18. Mahsa Shabani and Sami Yilmaz, 'Lawfulness in Secondary Use of Health Data: Interplay between Three Regulatory Frameworks of GDPR, DGA & EHDS', *Technology and Regulation*, (2022), 128–34 https://doi.org/10.26116/techreg.2022.013.

scope of this paper,[19] some of them provide useful illustrations of the difficulties HDABs may be faced with. Taking article 53 for example, it relates to contexts such as 'scientific research'[20], to support public sector bodies or Union institutions, agencies and bodies, including regulatory authorities, in the health or care sector to carry out their tasks defined in their mandates',[21] for boosting innovation in these sectors and for 'innovation activities for products or services contributing to public health or social security'. Some of these potential grounds for being granted an access permit are noticeably very wide.

'Scientific research' is a notoriously broad term for example. The concept is not itself defined within the EHDS regulation. Elsewhere the potential breadth of this notion is well illustrated, for example by its broad definition within the GDPR (i.e. with boundaries that are arguably difficult to define concisely).[22] Determining what 'scientific research' is will accordingly require complex case by case deliberation. The need to foster scientific research is used a number of times in the recitals of the regulation to justify its existence. Whilst not defining the concept, the EHDS regulation does limit the areas for whicha data access permit should be granted to certain areas, though these are notably wide in nature. This includes:[23]

> "Research in the health or care sectors, ...contributing to public health or health technology assessment, or ensuring high levels of quality and safety of health care, of medicinal products or of medical devices, with the aim of benefitting the end-users, such as patients, health professionals and health administrators, including... (i) development and innovation activities for products or services; (ii) training, testing and evaluating of algorithms, including in medical devices, invitro diagnostic medical devices, AI systems and digital health applications... "

Despite these precisions, there should be no doubt that the scope for granting a data access permit under this ground is extremely wide. Not only are the contexts themselves very broad, but the general understanding of what can constitute scientific research in each of this contexts is very expansive. As recital 61 of the EHDS text states:

> "The provision of the data should also support activities related to scientific research. The notion of scientific research purposes should be interpreted in a broad manner, including technological development and demonstration, fundamental research, applied research and privately funded research. Activities related to scientific research include innovation activities such as training of AI algorithms that could be used in healthcare or the care of natural persons, as well as the evaluation and further development of existing algorithms and products for such purposes."

'Innovation' is a notably broad term that is not defined with the EHDS Regulation. This formulation for granting a data license, seemingly goes even beyond the classical vision of what scientific research is. It encompasses activities that are more readily categorised as innovation activities i.e. related to the improvement of medical devices or products. Those familiar with the definition of 'scientific research'within the GDPR might therefore wonder what the limits of this concept are given that the notion of scientific

19. The author of this paper has done this elsewhere recently with colleagues. See: P Quinn, C Yao, E, Eylne (2024)Limits to Health Data Access Body Discretion and a Need to Comply with the GDPR – Enough to Protect Against Improper Sharing of Health Data Through the EHDS? Computer Law & Security Review (Accepted after review, awaiting publication)
20. Article 53(1)(e)
21. Article 53(1)(b)
22. The European Data Protection Supervisor has provided some guidance that arguably reduces the breadth of what can be construed as "scientific research" under the GDPR. See: European Data Supervisor, "A Preliminary Opinion on data protection and scientific research", 6 January 2020
23. EHDS Regulation 51(e)

research withing the GDPR was already noticeably broad.[24] Unfortunately at present the EHDS Regulation itself provides limited guidance on any potential limitation of the concept of 'innovation'.[25]

A similar point can be made concerning the possibility outlined in article 53(1)(b) of providing electronic health data in order to *"support public sector bodies or Union institutions, agencies and bodies including regulatory authorities, in the health or care sector to carry out their tasks defined in their mandates"*. Two factors make this a potentially wide-ranging possibility to grant data licenses;*First*, the concept of 'public bodies in the health or social sector' itself is extremely wide. A number of factors contribute to this. Notably, the concept of public bodies is seen as including not only entities at the national but also the EU level. The purposes for which such entities use the data they receive are also not defined, the sole restriction being that they use it in line with their "mandates" and that the public bodies in question be in the "health or social sector". Given the enormous range of public bodies that exist within the health and social sectors and the tasks they carry out, the EHDS regulation entails making electronic health data available for a range of purposes that are very difficult, if not impossible to define. Most strikingly the terms' health sector' or 'social sector' are not defined in the the EHDS regulation.[26] The drafters appear therefore to leave the discretion in determining which entities are in the health and social sector to the discretion of the Health Data Access Bodies. They will presumably be guided by how such bodies are recognized under national law according to their 'mandates'. *Second*, the notion of what a 'mandate' is, is also not defined or restricted. It seems that a mandate may be for anything so long as it is somehow connected to the health and social care sector. Not only do the types of entities in these sectors vary enormously, but so too will the functions they carry out. Certain activities may be classified as healthcare in one Member state but not in another.[27] The same is true for the social sector which may vary enormously, with public entities having far wider mandates in some states compared to others.[28] In some states, such activities may be largely public whilst in others they may be to a lesser or greater extent commercialized.[29] Once again untangling this web of complexity will be a significant task for HDABs that will require not only the availability of expertise in terms of personnel, but also the resources to let them investigate the individual context of each data access permit request in detail.

4.2 Reasons not to grant a data access request (article 54)

In certain contexts a HDAB may be mandated to refuse a data access request, even though it seemingly falls within one of the criteria listed with article 53 of the EHDS proposal. This will occur when the proposed data processing falls within one of the forbidden categories listed within article 54. The categories are noteworthy in two principle regards.

24. Recital 157 of the GDPR for instance states ... "Where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research."
25. Recital 61 does however give some examples including " ...activities related to scientific research include innovation activities such as training of AI algorithms that could be used in healthcare or the care of natural persons, as well as the evaluation and further development of existing algorithms and products for such purposes..."
26. The author of this paper, together with a number of colleagues made representation to the LIBE committee of the European Parliament concerning this issue. Indeed in its recommendations the LIBE committee opined to expand the relevant provision (i.e. article 34(1)(e) providing more detail i.e. to " scientific research related to health or care sectors and relevant purposes, contributing to public health or social security, or ensuring high levels of quality and safety of health care, of medicinal products or of medical devices, with the aim to benefit the end-users of the activity, including:" See: "DRAFT REPORT on the proposal for a regulation of the European Parliament and of the Council on the European Health Data Space (COM(2022)0197 – C9-0167/2022 – 2022/0140(COD)) 10.2.2023" produced by the Committee on the Environment, Public Health and Food Safety Committee on Civil Liberties, Justice and Home Affairs
27. J. Schreyögg and others, 'Defining the "Health Benefit Basket" in Nine European Countries', *The European Journal of Health Economics*, 6.1 (2005), 2–10 https://doi.org/10.1007/s10198-005-0312-3.
28. Jacques Defourny and Marthe Nyssens, 'Social Enterprise in Europe: Recent Trends and Developments', *Social Enterprise Journal*, 4.3 (2008), 202–28 https://doi.org/10.1108/17508610810922703.
29. Jacques Defourny and Marthe Nyssens, 'Social Enterprise in Europe: At the Crossroads of Market, Public Policies and Third Sector', *Policy and Society*, FINANCING THE THIRD SECTOR, 29.3 (2010), 231–42 https://doi.org/10.1016/j.polsoc.2010.07.002.

First, in some instances, the areas where a health data access permit may not be granted are relatively clear. This includes in instances where the data will be used to discriminate against certain type of groups or individuals. As article 54(d) states, permits shall not be granted for:

> "developing products or services that may harm individuals, public health or societies at large, including, but not limited to illicit drugs, alcoholic beverages, tobacco and nicotine products, weaponry or products or services which are designed or modified in such a way that they create addiction or that they contravene public order or cause a risk for human health"

In other areas however, the proposed areas where a data license should not be provided are extremely broad. This can be illustrated for example with regards the context of taking decisions "detrimental to a natural person or a group of natural persons based on their electronic health data".. where such deciscions have "legal, social or economic, effects or similarly significantly affect those natural persons".[30] This appears to leave broad discretion to those responsible for granting data permits in determining what products or services would meet such criteria. In particular the notion of negative social effects is hard to delineate and will leave considerable room to HDAB's to employ their own particular interpretation (perhaps also being influenced from their respective national context).

Similarly Article 54(d) demands that a data access permit not be issued where the goal is to develop "products or services that may harm individuals, public health or societies at large, including, but not limited to illicit drugs, alcoholic beverages, tobacco and nicotine products, weaponry or products or services which are designed or modified in such a way that they create addiction or that they contravene public order or cause a risk for human health". Whilst some important examples are given, they are not exhaustive in nature. This means that HDABs may decide that other potential products or services may be cable of harming "individuals, public health or societies at large". This presents an enormous range of potential activties, a full analysis of which is beyond the scope of this paper. Once again, this will grant enormous discretion to HDABs and open the door to considerable variation at the national level concerning what consituions potneitally harmful products or services.

A *second* striking observation that can be made is that a number of exceptions outlined in article 54 would not be considered otherwise illegal. Indeed many for example may otherwise be permissible under the GDPR, national data protection law and other relevant frameworks. This may include a number of instances that are considered normal commercial practices. This certainly includes for instance use of secondary data for research within the insurance industry and in marketing.[31] It may also include a number of activities that could be considered capable of harming "individuals and societies at large". This concept seemingly could include a wide range of activities that are legal but may be considered harmful, not only for health based reasons but potentially also societally (e.g. where they may contribute to inequality amongst various groups in society).

The author of this paper would suggest therefore that the legislators of the EHDS regulation wanted to give HDABs obligation to make moral and ethical judgments that go beyond the strict letter of the law. This is arguably problematic for a number of reasons. One being that there is enormous variation across Europe in terms of public opinion as to what is considered to be ethically or morally acceptable with regards to the collection, processing and potential profit making from electronic health data.[32] Additionally, the EHDS proposal isnot very instructive about the extent to which HDABs should be informed at all by public opinion or whether their judgments should be on the basis of specific expertise (which can also vary to large extent across various cultures). One can hope that with the existence of the EHDS board and its mandate to issue guidance on best practices in the use of secondary data, uncertainty in this area will be reduced with time

30. EHDS proposal, Article 54(a).
31. Excluded underArticle 54(c) of the EHDS proposal
32. Piret Veerus, Joel Lexchin, and Elina Hemminki, 'Legislative Regulation and Ethical Governance of Medical Research in Different European Union Countries', *Journal of Medical Ethics*, 40.6 (2014), 409–13 https://doi.org/10.1136/medethics-2012-101282.

(though it may take some time for this to occur).[33] Another reason is that it is arguably concerning to compel (as article 54 of the EHDS seemingly does) HDABs to exercise their discretion in such a profound way when it uncertain how such discretion should be used or what the outcome will be. Questions of morality or general harms go beyond notions of physical or even privacy harms, that are arguably easier to agree upon in an objective manner. This raises serious questions about foreseeability of the decisions made by HDABs. Once again one can hope that such problems can be resolved with time through clear guidance by the EHDS board. Even where such guidance eventually exists the fact that enforcement of the EHDS rules will occur at the Member State level (i.e. through HDABs) will allow for a certain level of uncertainty and thus divergence to remain.[34] Even with good guidance however, deciding how to use this level of discretion will likely entail an intensive and resource demanding level of analysis on the part of HDABs in the various contexts in which data access permits are made.

5. HDABs will Ensure Key Elements of the GDPR are Adhered to.

HDABs must also ensure that some of the main tenets of the GDPR will be respected by the proposed processing operation in question. The EHDS Regulation accordingly states:[35]

> *"... Since the secondary use of health data involves the processing of personal data concerning health, the relevant provisions of Regulation (EU) 2016/679 apply and the supervisory authorities under Regulation (EU) 2016/679 and Regulation (EU) 2018/1725 should* remain the only authorities competent for *enforcing these rules."*

In doing so the EHDS also makes clear that all secondary processing of electronic health data provided by the EHDS must be compliant with the GDPR. For data recipients who have managed to obtain a data access permit from an HDAB, the GDPR will apply to any processing they perform on electronic health data (presuming it is of a personal nature).[36] Whilst, HDABs are required, where necessary to co-operate with data protection supervisory bodies to ensure this occurs, it does not appear that it is the role of HDABs to ensure that all potential requirements that the GDPR may pose in a particular context are complied with. This is because the proposal text only explicitly demands that HDABs check that several key requirements of the GDPR are being respected. These are the need to ensure that the potential recipient has a valid legal base under the GDPR, that the data processing principles of minimization and purpose limitation will be respected and that, where possible, any data provided is anonymized.[37] Whilst an explicit duty to ensure only that these aspects of the GDPR are complied withis obviously less onerous than a need to ensure compliance with all potentially applicable aspects, the demanding nature of this requirement should nonetheless not be understated. It should also not be forgotten that the EHDS framework appears to foresee that National Contact Points (on behalf of Member States) will be joint controllers of any personal data that is provided for processing in a secure environment.[38] One could presume (though this admittedly remains unclear) that NCPs will be guided by HDABs in carrying out their duties in this regard. Whilst it is beyond the scope of this paper to go through all potential requirements that might be applicable to HDABs as a result of this, it is clear that these will be important and entail further burdens upon HDABs to those. These burdens will apply in addition to the requirements which have been explicitly described by the EHDS regulation. Complying with these requirements will entail a serious commitment on the part of HDABs that

33. Article 94(1)(b) of the EHDS regulation states that the EHDS board shall "issuing written contributions and exchanging best practices on matters related to the coordination of the implementation at Member State level, taking into account the regional and local level, of this Regulation and of the delegated and implementing acts adopted pursuant to it"
34. 'Editorial: On Digital Sovereignty, New European Data Rules, and the Future of Free Data Flows by Svetlana Yakovleva :: SSRN' https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4320767 [accessed 28 February 2024]. On page 6 the author states: "While data-related rules introduced by each of the above-mentioned acts overlap, regulatory and enforcement authorities established by each of the acts will, at best, only coordinate at Member States level. This will lead to divergence in the interpretation and enforcement of these acts across the EU and possible forum-shopping."
35. Recital 65 of the EHDS proposal
36. Article 2(2)(c) states that "electronic health data' means personal or non-personal electronic health data"
37. Article 66 and 68 of the EHDS regulation
38. Article 75(10) of the EHDS regulation

will require significant resources to execute correctly (especially in a context where a HDAB is receiving many requests). Some of the main issues relating to this are outlined below.

5.1 Legal Base

The first of these major requirements in the need to ensure a legal base exists for the proposed processing.[39] As recital 52 of the proposal states:

> *"For the purpose of processing electronic health data for secondary use, one of the legal bases referred to in Article 6(1), points (a), (c), (e) or (f), of Regulation (EU) 2016/679 in conjunction with Article 9(2) thereof is required"*

Compliance with this requirement must be demonstrated in the health data access application that potential data recipients must address to the relevant HDAB.[40] Health Data Access Bodies will seemingly have to ensure not only that potential data recipients have identified a legal base that covers their proposed processing, but also in many instances that it meets requirements in national law also. This will be for example the case where data controllers claim to be processing for reasons of public interest. In such instances the GDPR is clear that data controllers must also point to relevant law at EU or Member State level.[41] This latter requirement means that unless data controllers meet the requirements posed by national lawthat are applicable to their particular processing context they cannot be considered to have a valid legal basis for processing as required by the GDPR (which will usually be required for most forms of likely applicable legal base).[42]

Assessing the validity of a legal basis that is presented on a health data access permit is likely to be a more complex and time-consuming endeavour than might appear to be the case at first glance. Far from being a mere tick box exercise, doing so in the context of secondary health data access requests is likely to be a demanding exercise. Two factors will make deliberations in this area a complex process that will demand a certain level of reflection. The *first* is the need to assess whether a particular legal base is indeed suitable for use in the processing context that is being proposed. The *second* relates to the need to assess potential compatibility with relevant Member State law. Some of the difficulties these requirements will pose for HDAB's are illustrated below.

5.1.1 Assessing the Intrinsic Suitability of a Particular legal base

The first can be thought of as the need to determine the intrinsic suitability of the type of base that has been selected. This reflects a need to anlayse whether a proposed processing operation really can be squared with the legal base that has been provided with a data access request. Part of this problem arises because the terminology used in the GDPR is sometimes rather broad and open to interpretation. This can be well illustrated for example with the term 'scientific research'. The notion of scientific research outlined in the GDPR is notoriously broad. As section 4.A of this paper discussed (with reference to recital 61 of the EHDS regulation), the drafters of the EHDS regulation seemingly envisaged a similarly broad concept. In this context a major problem for HDABs will be in determining whether an instance of proposed processing actually falls within such a wide ground or not, especially given that its conceptual limits may not be clear. In the case of 'scientific research' some useful advice (in terms of delineating the concept) was provided by the European Data Protection Supervisor when it stated:

---

39. As recital 52 clarifies, that the EHDS regulation itself will provide a legal basis for the HDAB to make electronic health data available for secondary processing, stating *inter alia*: "this Regulation also assigns tasks in the public interest within the meaning of Article 6(1), point (e), of Regulation (EU) 2016/679 to the health data access bodies, and meets the requirements of Article 9(2), points (g) to (j), as applicable, of that Regulation. If the health data user relies upon a legal basis set out in Article 6(1), point (e) or (f), of Regulation (EU) 2016/679, this Regulation should provide for the safeguards required under Article 9(2) of Regulation (EU) 2016/679"
40. Article 68 of the EHDS proposal
41. This is also confirmed for the relevant legal bases in article 9 GDPR that will apply in the (seemingly frequent) case that the data in question is sensitive data. This is the case for example with the public health base (article 9(2)(i) or the scientific research base (article 9(2)(j).
42. Giulia Schneider, 'Disentangling Health Data Networks: A Critical Analysis of Articles 9(2) and 89 GDPR', *International Data Privacy Law*, 9.4 (2019), 253–71 https://doi.org/10.1093/idpl/ipz015.

> "*Scientific research applies the 'scientific method' of observing phenomena, formulating and testing a hypothesis for those phenomena, and concluding as to the validity of the hypothesis.... The conduct of research must allow testing of hypotheses, with both the conclusion and the reasoning transparent and open to criticism. Openness and transparency help distinguish between science and pseudo-science*." ... "[43]

The comments made by the EDPS indicate that there should be a clear limit as to what can be understood as constituting scientific research. They also appear to offer a narrower vision of the concept than might initially be apparent in the relevant recitals of the GDPR. [44] *Inter alia* such a position seems to demand the presence of what might traditionally be known as the 'scientific method'. This may for example include the use of the empirical method whereby a proposed theory is tested against the available evidence.[45] Whatever the precise delimitation of the concept of scientific research, it seems likely that HBABs will have to investigate the specific context in which scientific research is indeed put forward as a legitimate data processing base under the GDPR. It is only through such enquiry that HDAB's will be able to determine whether the invocation of this base is legitimate or not.

Whilst it is beyond the scope of this paper to perform a full analysis of the breadth of all legal bases found within the GDPR the author of this paper would argue that a similar point could be made for potential use of the 'public health' [46]or the 'manifestly made public' base.[47] The latter[48] in particular requires significant deliberation to determine whether the conditions required to use the base have been met or not.These include a potential analysis of the legitimate expectations of data subjects at the time they made their data public. Once again this will require and considerable level of context-based deliberation that will demand both a command of the facts in a particular case and also the knowledge and ability to apply the law in that particular context.[49]

5.1.2 Assessing Compatibility with National Law

The second major difficulty will relate to the need to be aware of and understands the high level of potential variation that exists in potentially applicably Member State law. Whist the GDPR in general has a harmonizing effect for laws relating to personal data, for health data this effect is less pronounced. This is because, as outlined in article 9(4) of the regulation, the GDPR permits Member States to maintain divergent laws related to health, genetic or biometric data.[50] Given that each of these types of data may be in demand through the EHDS as 'electronic health data,' HDABs will have to take into account in a wide range of instances where national law may pose further conditions on the processing of electronic health data.[51]

---

43. European Data Supervisor, "A Preliminary Opinion on data protection and scientific research", 6 January 2020, p.10.
44. This could seemingly exclude some forms of commercial activity that could potentially fall the broader notion of scientific research alluded to in the GDPR.Interestingly, it would also appear to preclude some of the contexts under Article 53 EHDS for which a data access permit should be granted. This might potentially include 'development and innovation activities for products or services' or for the 'training, testing and evaluating of algorithms' (Article 53 (1)(e)).
45. Johan Galtung, 'Empiricism, Criticism, Constructivism', *Synthese*, 24.3 (1972), 343–72 https://doi.org/10.1007/BF00413652.
46. GDPR article 9(2)(j)
47. The author conducted a more in depth analysis of these bases in a recent paper: Paul Quinn, 'Research under the GDPR - a Level Playing Field for Public and Private Sector Research?', *Life Sciences, Society and Policy*, 17.1 (2021), 4 https://doi.org/10.1186/s40504-021-00111-z.
48. GDPR article 9(2)(e)
49. For more on this see EDPB document "Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR" Adopted on 8 October 2024, available at: https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf
50. Fruzsina Molnár-Gábor and others, 'Harmonization after the GDPR? Divergences in the Rules for Genetic and Health Data Sharing in Four Member States and Ways to Overcome Them by EU Measures: Insights from Germany, Greece, Latvia and Sweden', *Seminars in Cancer Biology*, Precision Medicine in Cancer, 84 (2022), 271–83 https://doi.org/10.1016/j.semcancer.2021.12.001.
51. The EHDS regulation does notably limit the application of some forms of national law in this area, notably where such laws demand that consent be given before health data is processed. See Recital 52 which states: "Consequently, Member States should no longer be able to maintain or introduce under Article 9(4) of Regulation (EU) 2016/679 further conditions, including limitations and specific provisions requesting the consent of natural persons, with regard to the processing for secondary use of personal electronic health data under this Regulation, with the exception of the introduction of stricter measures and additional safeguards at national level aimed at safeguarding the sensitivity and value of certain data as laid down in this Regulation."

One such area relates to the number of potentially applicable legal bases under the GDPR requiring accompanying Member State law.[52] This is the case for example with the public interest base under article 6 and more specifically the 'public health' and 'scientific research' bases that out outlined in Article 9 and which are relevant to sensitive data.[53] Unfortunately for HDABs, ensuring such a correct legal basis exists may not be a simple task. The variation in legislation at the national level in this area remains significant. Not only do Member States have different legislation but the form and scope of such legislation may be highly variable.[54] Legal frameworks that for instance relate to who can process data for the purposes of scientific research may vary greatly.[55] Some Member States may for example have very general legal frameworks that will provide legal bases to scientific research for a wide variety of purposes whilst other may relate to processing in more specific areas or to specific types of data (e.g. genetic data).[56] Similarly, some legal frameworks may be related to all types of entities that wish to process a particular form of data or for a particular reason. In other instances legislation may only provide cover for certain forms of institutions (e.g. public sector bodies, universities or biobanks).[57] The extent to which commercially motivated research will fall under such exceptions is also likely to vary.[58]

The upshot of this variability is that unless the relevant individual(s) carrying outan assessment on behalf of an HDAB is familiar with the relevant framework in a particular Member State, a significant level of research may be required. Whilst one might expect those working for HDABs to be familiar with their own legal framework, one can not expect them to be familiar with potentially applicable legal requirements in many or even most Member States. This point will be extremely pertinent given the text of the EHDS makes it clear that HDABS not only shouldconsider requests from other jurisdictions in Europe but should not discriminate between them and requests made in their own jurisdiction.[59] Given this, those working for HDABs will have to either possesses a familiarity with the legal systems of many Member States (which seems unlikely), or the time and ability to be able to interrogate unfamiliar national frameworks to see if the legal basis that has been put forward on a data access applications is indeed valid. In Ireland for

52. Regina Becker and others, 'Purpose Definition as a Crucial Step for Determining the Legal Basis under the GDPR: Implications for Scientific Research', *Journal of Law and the Biosciences*, 11.1 (2024), lsae001 https://doi.org/10.1093/jlb/lsae001.

53. Articles 9(2)(i) and 9(2)(j) respectively

54. Marko Hölbl, Boštjan Kežmah, and Marko Kompara, 'Data Protection Heterogeneity in the European Union', *Applied Sciences*, 11.22 (2021), 10912 https://doi.org/10.3390/app112210912.

55. Quinn, 'Research under the GDPR - a Level Playing Field for Public and Private Sector Research?'

56. Katarzyna Kolasa and others, 'Future of Data Analytics in the Era of the General Data Protection Regulation in Europe', *PharmacoEconomics*, 38.10 (2020), 1021–29 https://doi.org/10.1007/s40273-020-00927-1.

57. For a good overview see report "Assessment of the EU Member States' rules on health data in the light of GDPR Specific Contract No SC 2019 70 02 in the context of the Single Framework Contract Chafea/2018/Health/03" which states on p 60 "The results of the legal survey indicate that 9 Member States were reported as not having adopted sectoral legislation. Of the 18 Member States who were reported as having such legislation, there are variances in safeguards applied (see Table 5.1). Where a Member State is listed as not having sectoral legislation in place to address the use of data for research, this does not imply that data cannot be used in line with Article 9(2)(j) at all, it may mean that the provisions for such use are included in the general data protection legislation that has been implemented in pursuance of the GDPR".Ireland is an example of a state that has complex sectoral legislation.. The Netherlands is an example of a country that does not. For more on the latter see: Irith Kist, 'Assessment of the Dutch Rules on Health Data in the Light of the GDPR', European Journal of Health Law, 30.3 (2022), 322–44 https://doi.org/10.1163/15718093-bja10096.

58. As this author commented in another paper "Whilst it is of course possible that some forms of commercially motivated forms of scientific research will be in the public interest (e.g. pharmaceutical research), it is likely that most forms will not be able to meet such a test. Others may even require approval of specialist committees (e.g. Ireland)... Whilst there are certain exceptions, the general rule of thumb is that it will be more difficult for private or commercial entities to avail themselves of 'the research exception' outlined in the GDPR." See: Quinn, 'Research under the GDPR - a Level Playing Field for Public and Private Sector Research?' For more on the public interest requirement see: Edward S Dove and Jiahong Chen, 'Should Consent for Data Processing Be Privileged in Health Research? A Comparative Legal Analysis', International Data Privacy Law, 10.2 (2020), 117–31 https://doi.org/10.1093/idpl/ipz023. On p8-10 the authors discuss how under Irish law data controllers must seek permission from the minister of Health who will issue a decision *vis-à-vis* an appointed committee. An application must be accompanied by "written information demonstrating that the public interest in carrying out the health research significantly outweighs the public interest in requiring the explicit consent of the data subject under Regulation 3(1)(e) together with a statement setting out the reasons why it is not proposed to seek the consent of the data subject for the purposes of the health research."

59. Recital 74 of the EHDS regulation states " As their resources are limited, health data access bodies should be allowed to apply prioritisation rules, for instance prioritising public institutions over private entities, but they should not discriminate between the national organisations and organisations from other Member States within the same category of priorities..."

example "a researcher may need to refer to general data protection law, sectoral law, and may also need to read such laws alongside authoritative guidance which addresses use of data for research".[60] Ireland is not unique in this situation, meaning that HDABs may frequently be expected to perform such complex analyses alongside the other assessments that are outlined in this paper. It should be pointed out that difficulties in this area may be somewhat alleviated were HDABs in different states to work effectively with each other. Indeed the EHDS is clear that it expects HDABs to "co-operate closely with each other".[61] Whist this is an important factor that should not be ignored, the author of this paper would suggest that the need to resort to and co-ordinate such collaboration (where it does indeed function well) will nonetheless represent a significant administrative burden.

5.2 Data Processing Principles

The EHDS proposal also explicitly states that HDABs must ensure that the data processing principles of 'minimization' and 'purpose limitation' are respected.[62] These are two of the core processing principles outlined within the GDPR that should be applied to all forms of processing of personal data. The former ensures entailing that only the minimum amount and types of personal data are used in any particular instance of processing. The latter ensures that personal data is only processed for the reasons that was initially intended when the data was obtained. Although the existence of such principles is described in highly abstract terms by both the GDPR and the EHDS Regulation, their application in reality will require careful and considered application in each particular context, in many cases demanding a high level of expertise in the specific area the processing relates to. Whilst the concept of data minimization for example may appear abstract and even simple when read in a standalone manner in the text of the GDPR, the reality is that discerning what this requirement demands in a particular context can be quite demanding.

The data processing principles are requirements that must not only be considered in the light of a particular processing context, but also the other data processing principles.[63]In terms of the former, this requires considering not only the aims of the processing operation in question but also to understand the nature of the processing itself. Without doing this it is impossible to be able to make any assessment about what data may be required or not.[64] In terms of the latter, it is necessary to consider also principles such as accuracy and storage limitation. Trying to understand what a requirement such as minimization might mean in isolation from the requirements other processing principles (which commonly require a form of 'trade-off') will often be meaningless.[65] This arguably means that although the EHDS proposal does not explicitly demand HDABs to consider other data processing principles (outside of data minimalization and purpose limitation), they will often be required to do so in reality.

Both factors means that the need to determine what constitutes data minimization in a particular context will be far from simple in reality. Whilst one could make the argument that, given that the EHDS regulation itself is sector specific (i.e. applying to 'electronic health data'), these problems will be somewhat minimized, the author of this article would suggest this effect will be of a minimal nature. This is because of the diverse nature of what can constitute secondary health data. Whilst the regulation may itself as being sectoral in nature, the reality is that it is capable of encompassing an incredibly diverse array of data coming from very different contexts. Ensuring requirements such as purpose limitation and minimization are met will, in reality, require expertise in the particular area of secondary health data proposed.What data

60. "Assessment of the EU Member States' rules on health data in the light of GDPR Specific Contract No SC 2019 70 02 in the context of the Single Framework Contract Chafea/2018/Health/03" p 60
61. Article 37(1)(o) of the EHDS regulation
62. EHDS regulation Article 66
63. Ingo Siegert and others, 'Personal Data Protection and Academia: GDPR Issues and Multi-Modal Data-Collections', *Online Journal of Applied Knowledge Management (OJAKM)*, 8.1 (2020), 16–31 https://doi.org/10.36965/OJAKM.2020.8(1)16-31.
64. It has also long been recognized that some of the principles can be read as required conflicting things. This means that it is necessary to consider data processing principles together at the same time in a holistic manner requiring some level of compromise between them. See for example: Tal Z. Zarsky, 'Incompatible: The GDPR in the Age of Big Data', *Seton Hall Law Review*, 47.4 (2016), 995–1020.
65. Asia J. Biega and Michèle Finck, 'Reviving Purpose Limitation and Data Minimisation in Data-Driven Systems', *Technology and Regulation*, 2021, 44-61 Pages https://doi.org/10.26116/techreg.2021.004.

minimization means for example in an area such as genomics[66] may be very different than in research into MRI images of potential cancers.[67] In the former for example the HDAB will need to understand whether whole genome (i.e. GWAS) sequences are needed or not,what data from how many individuals is required and what complimentary data (e.g. from electronic health records) may be necessary to achieve the desired result. Without a minimum level of experience and familiarity with such matters it will arguably be difficult to perform a meaningful assessment of what data minimization actually entails in each particular context.

A similar point can also be made about the need to assess purpose limitation. Once again this principle cannot be considered in isolation but must be considered together with other relevant and related principles. As with the concept of minimization, an awareness of both the specific context and the wider domain of processing may often be necessary to determine what types of processing activities can be considered as falling under a given purpose. Some forms of research may for instance be highly iterative, where the research question itself may be refined during research. Indeed the increased use of AI in scientific research means that older concepts of research construction (where the precise goal and research questions are known before the research commences) are arguably becoming outdated.[68] All of these factors will once again mean that HDABs will have to perform a challenging role in this area where each dossier is likely to require a considerable amount of reflection.

5.3 The Need to Use Anonymised Data (where possible).

HDABs should also, where feasible, ensure data provided to data recipients is anonymous. The EHDS proposals states:[69]

> "The health data access bodies shall provide the electronic health data in an anonymised format, where the purpose of processing by the health data user can be achieved with such data, taking into account the information provided by the health data user."

This requirement implies yet another form of complex analysis that must be required by HDABS. This analysis can be broken down into two component tasks. These relate to the need to need to discern what constitutes anonymity in a particular context and deciding when it should be permissible to use non-anonymised data. These are further discussed below.

5.3.1 Deciding What Constitutes Anonymity in a Particular Context

As with other determinations around the concept of personal data this is once again both complex and very context dependent. It beyond the scope of this paper to explore this question in full depth,[70] but as deliberations elsewhere have demonstrated, the answer to the question of what constitutes anonymity is both not only highly contextual but one that is, by its nature, ever evolving.[71] Given the lack of definitive case law on this subject, much importance is put on academic writings and expert opinion. The most relevant of these (i.e. an article 29 working party opinion)[72] is seen as becoming rather dated given technological

66. Quinn, 'Research under the GDPR - a Level Playing Field for Public and Private Sector Research?'
67. Damian Eke and others, 'Pseudonymisation of Neuroimages and Data Protection: *Increasing Access to Data While Retaining Scientific Utility*', *Neuroimage: Reports*, 1.4 (2021), 100053 https://doi.org/10.1016/j.ynirp.2021.100053.
68. Janos Meszaros and Chih-hsing Ho, 'AI Research and Data Protection: Can the Same Rules Apply for Commercial and Academic Research under the GDPR?', *Computer Law & Security Review*, 41 (2021), 105532 https://doi.org/10.1016/j.clsr.2021.105532.
69. EHDS Regulation Article 66(2)
70. The author dealt with these issues in an older paper: Paul Quinn, 'The Anonymisation of Research Data—A Pyric Victory for Privacy That Should Not Be Pushed Too Hard by the EU Data Protection Framework?', *European Journal of Health Law*, 24.4 (2017), 347–67.
71. Perhaps the most important court judgement of the case thus far has been Case C-582/14, Patrick Breyer v Bundesrepublik Deutschland, [2016], ECLI: EU: C: 2016:779. Whilst instrustive, it is not clear how far the the reasonning of the case can be read beyond the specific context of that case (i.e. relating to the non-anonymity of IP addresses). For an interesting blog on this dicussion Please read: "ANONYMITY IS IN THE EYE OF THE BEHOLDER... OR IS IT?" By Karen Cruyt, 1st December 2023, available at: https://hall.research.vub.be/anonymity-is-in-the-eye-of-the-beholder-or-is-it
72. Article 29 Working Party (A29 WP), 'Opinion 05/2014 on Anonymisation Techniques' (10 April 2014) WP 216.

advances, with calls for a more pragmatic approach to the concept arguably gaining ground.[73]In any event, various discussions on what is needed to ensure anonymity often focus on three key factors.

The *first* is the intrinsic identifiability of such data. This relates to the type of data and its volume. If it includes obvious identifiers such as names and social security numbers, the data is self evidently personal in nature. Even data elements that are not of such a directly identifiable nature may permit identification if present in a particular manner or if it is present with the necessary complimentary data. The size of the dataset may also be relevant. The bigger the dataset is the more likely that various processes can link it to specific individuals. (e.g. big data processing). These factors must be considered alongside a *second* important criteria i.e. what forms of potentially complimentary data are available to a data recipient.[74] In doing so it is necessary to ask does it have further data in its possession or is there other data available that could allow the data to be personalized? *Third*, it is necessary (taking into the technological state of the art) to determine if the if the potential recipient has the means to identify individuals. In an age where computing prowess and the resultant algorithmic power is ever increasing, this is no simple task.[75] Once again, analyzing these factors will represent a formidable demand for HDABs.

5.3.2 Deciding when it is permissible to use personal data?

Whilst the EHDS stipulates that where possible anonymous data should be provided to data recipients, it is also clear that where necessary personal data can be provided (in a pseudonymised format).[76] This can occur where it is necessary to have personal data to perform the proposed processing function and there are sufficient safeguards for doing so. Again, deciding upon these matters will require careful deliberation on the part of HDABs. In many instances anonymous data will not be useful to scientific researchers given that in order to be anonymous it would be necessary to remove data elements that may be useful to the research in question (e.g. socio-economic factors).[77] Determining when this is the case will once again require a knowledge and an understanding of both the field of research and the particular processing operation in question. The same is also true concerning the security measures that should be enacted where it is deemed acceptable to process personal data. It seems unlikely that HDABs will be able to use standard security measures that would be capable of applying to all circumstances. On the contrary, it is more probable that they will have to formulated upon the basis on contextually informed expertise on a case-by-case basis. This will further add to the complexity of the analysis expected on the part of HDABs and their potential workload.

6. A Need to Affirm Ethical Scrutiny

HDABs also appear to be given an important role to ensure that ethical issues surrounding a potential data access permit have been scrutinized. This can be seen in a number of ways. First, according to article 54 of the regulation, HDABS must (as is discussed above in more detail section 3) not allow proposed data use that would have a harmful effects on individuals or society. Second. HDABs must seemingly ensure that, where necessary, they determine that the proposed processing in question has been the subject of ethical scrutiny, *inter alia* by any relevant ethical commissions. Whilst the EHDS proposal does not make HDABs themselves responsible for performing a full ethical analysis, it does make them responsible for ensuring that such an analysis has been performed in accordance with relevant national law.[78]Article 67 of the regulation states that HDABS should use such information when assessing the validity of data access applications.

73. Daniel Groos and Evert-Ben van Veen, 'Anonymised Data and the Rule of Law', *European Data Protection Law Review*, 6.4 (2020), 498–508 https://doi.org/10.21552/edpl/2020/4/6.

74. In Breyer the court for instance stated that it was necessary to consider all complimentary data which the potential data controller had legal access to. The limits of the concept of 'legal access' remain unclear beyond the facts of this case however.

75. For more on this discussion see: Quinn P, Malgieri G. The Difficulty of Defining Sensitive Data—The Concept of Sensitive Data in the EU Data Protection Framework. German Law Journal. 2021;22(8):1583-1612. doi:10.1017/glj.2021.79

76. This is made clear *inter alia* in article 66 of the EHDS regulation.

77. Groos and Veen (n. 73).

78. Article 67 (2)(j) of the EHDS regulation requires that those demanding an access permit are responsible for providing "where applicable, information on any assessment of ethical aspects of the processing, required under national law, which may serve to replace the health data applicant's own ethics assessment."

Once again, these requirements introduce a considerable investigative burden on HDABs. This will be in determining what forms of ethical assessment potential data recipients should undergo at their respective national level. The level of heterogeneity in this regards is extreme.[79] Unlike national laws on the use of health data (which are also heterogenous)[80] there is no partially harmonizing legislation at the European level concerning how ethical reviews should be conducted (as there is with the GDPR for example)[81]. As a result, systems of ethical review (e.g. for scientific research), have evolved organically and in different ways across the many member states in Europe. This divergence can be seen in three ways.

First, the actual composition of the ethical review net in various countries differs greatly. In some countries (e.g. the Netherlands), such processes may be highly centralized. This may involve a small amount of ethics commissions that have oversight of large sectors or even several sectors.[82] In other countries (e.g. Belgium) ethical oversight may occur in a far more *ad hoc* and diverse manner.[83] In such contexts individual institutions (e.g. hospitals, university and large research institutions) may have their own respective ethics commissions. Given this, it may be difficult for outsiders, not familiar with such systems to understand who the key players are.[84]*Second*, the nature and source of legal authority with which such ethical commissions are vested with may vary greatly. This pertains both to the competence of such bodies (i.e. dictating the contexts when ethical review must be sought) and their respective composition (i.e. dictating who should sit on such bodies and what competences they may have). Again in some states such bodies may be described in national legislation whilst in others this may not be the case. In the latter category for example the role of ethics bodies may be outlined in the constitutive documents of particular organizations (e.g. universities, hospitals etc.) or may linked to funding requirements (e.g. funding linked to research).

This environment can create a very high level of heterogeneity where the nature of ethics bodies may vary not only from Member State to Member State but between regions, sectors and even different institutions. Expecting HDABs to be aware of such requirements andknow whether data permit applicants have complied with them may in such a context seem unrealistic. The fact that HDABs will be required to respond to data access requests from different Member States will complicate this picture further. The author of this paper would argue that it is a seemingly impossible task to expect HDABs to understand in detail the picture as it applies across Europe in the various Member States. Indeed, at present the author would argue that there is no single expert at present who possesses such knowledge. Expecting all HDABs to have staff that are capable of doing this would therefore seem to be asking the impossible. This raises serious questions of how it can be HDABs can be expected to perform their expected tasks in this regard. Whilst (as discussed above in section 5), the EHDS regulation demands that different HDABs co-operate where necessary,[85] the

79. Dirk Lanzerath, 'Research Ethics and Research Ethics Committees in Europe', in *Medical Research Ethics: Challenges in the 21st Century*, ed. by Tomas Zima and David N. Weisstub (Springer Verlag, 2022), pp. 423–39.

80. Hölbl, Kežmah, and Kompara.

81. Lanzerath (n 79). EU legislation does contain some references to ethics comittees. "In 2001, the "EU Directive 2001/20 EC" therefore came into force for the field of pharmaceutical research. This directive very explicitly requires the vote of an ethics committee. The Directive defines in Article 2 (k) an "Ethics Committee" as an "an independent body in a Member State, consisting of healthcare professionals and non-medical members, whose responsibility it is to protect the rights, safety and wellbeing of human subjects involved in a trial and to provide public assurance of that protection, by, among other things, expressing an opinion on the trial protocol, the suitability of the investigators and the adequacy of facilities, and on the methods and documents to be used to inform trial subjects and obtain their informed consent" There is also reference to the need for ethics review in Regulation (EU) No. 536/2014 on Clinical Trials on Medicinal Products for Human Use and Repealing Directive 2001/20/EC though the regulation does not outline how such review should occur. For more see Silvia Tusino and Maria Furfaro, 'Rethinking the Role of Research Ethics Committees in the Light of Regulation (EU) No 536/2014 on Clinical Trials and the COVID-19 Pandemic', British Journal of Clinical Pharmacology, 88.1 (2022), 40–46 https://doi.org/10.1111/bcp.14871.

82. R. IJkema and others, 'Ethical Review of COVID-19 Research in the Netherlands; a Mixed-Method Evaluation among Medical Research Ethics Committees and Investigators', *PLOS ONE*, 16.7 (2021), e0255040 https://doi.org/10.1371/journal.pone.0255040. "The Netherlands has 17 accredited Medical Research Ethics Committees (MRECs) that review medical research with human subjects [2]. Each MREC consists of legally mandatory disciplines (physician, paediatrician, legal expert, methodologist, ethicist, lay member, medical devices expert, clinical pharmacologist, pharmacist) supplemented by other members. Pursuant to the Dutch General Administrative Law Act"

83. For a good discussion (in Dutch only) on the historical development of ethics committies in Belgium see: Paul Schotsmans, M. Roelandt, and J. Stiennon, 'Lokale Commissies Voor Ethiek En Medische Praktijk', 2006 https://lirias.kuleuven.be/1948247?limo=0 [accessed 13 March 2024].

84. Luca Marelli and others, 'The European Health Data Space: Too Big to Succeed?', *Health Policy (Amsterdam, Netherlands)*, 135 (2023), 104861 https://doi.org/10.1016/j.healthpol.2023.104861.

85. Article 37(1)(o)

realities of requesting and engaging in such co-operation will no doubt invoke their own complexities to add this this picture.

7. A High Volume of Complex Decision making to be Required?

7.1 Are we expecting the impossible of HDABs?

The foregoing sections of this paper set out a series of complex investigations HDABs must undertake as part of their mandate under the EHDS. It is important not to view these requirements individually however, but as a collective whole given that these issues will need to be decided upon almost simultaneously in the context of a data access permit request. Indeed, the EHDS is clear that such requests should be dealt with swiftly, stipulating that they should be handled within 3 months.[86]The reality is that some HDABs may receive many applications and from all over Europe. Indeed, the EHDS not only foresees such a possibility but clearly encourages it by prohibiting HDABs from discriminating between data access permit requests from other Member States. As recital 74 of the EHDS regulation states:

> "As their resources are limited, health data access bodies should be allowed to apply prioritisation rules, for instance prioritising public institutions over private entities, but they should not discriminate between the national organisations and organisations from other Member States within the same category of priorities..."

In a European context where HDABs can receive data access requests from all over Europe, it seems likely that some may be more popular than others. Some HDABs may have better electronic health data catalogues than others making them a particularly appealing choice for data access permits. This may be particularly the case in Member States where there already exist advanced infrastructures permitting the sharing of secondary electronic health data. Given this there exists the potential for in demand HDABs to potentially be inundated with requests.

In such a situation it seems likely that some HDABs will have a range of complex organizational challenges linked to the quality and quantity of expertise they can deploy to the assessment of such dossiers. This is a result of the challenges posed not only by the potential quantity of applications which HDABs may receive, but also complexity of the various determinations they must make (many of which have been discussed in the various sections of this paper). In order to do this the author of this paper would argue that HDABs will need to be incredibly well resourced in both the 'depth' and 'quantity' of expertise they would need to possess. Indeed, the extent of these requirements would, it is submitted, make them difficulty to fulfil in reality. Each of these problems is explored further below.

7.1.1 Depth of Expertise

In the environment discussed above, HDABS will evidently need to possess personnel with an extremely eclectic range of talents. The previous sections of this paper have discussed the complex calls that must be made. These are in a range of areas spanning from, public policy, ethics/ethical oversight and data protection issues (not limited to an expertise at the European level but also at the national level).In addition, HDABs will similarly need staff that have a sufficient level of expertise to be able to understand the processing backgrounds in question. This includes not only a potentially wide range of scientific and technical domains but also ability to apply such knowledge in different contexts. Without such expertise it is unclear how an HDAB could expect to make the various assessments which it is tasked with. Given that it is unlikely any one individual will process all of this expertise it is likely that HDABS will have to have a portfolio of expertise at their disposal. This will likely take the form of various staff with a diverse background. The complexity of the assessments which HDABs must perform will likely mean that several

86. EHDS regulation Article 68(4). The health data access body may extend the period for responding to a data access application by 3 additional months where necessary, taking into account the urgency and complexity of the request and the volume of requests submitted for decision.

personnel with various expertise may have to consider a single dossier in order to deliberate on various facets it may possess. This further accentuates the problems outlined in this paper.

7.1.2 Quantity of Expertise

Given that HDABs will have to deliberate over a potentially large number of dossiers within fixed time constraints it seems likely that in order to fulfill their obligations they will also need to possess the relevant breadth of expertise outlined above in sufficient quantity. Having one expert on the nature of genetic data may for example be insufficient if the HDAB in question is receiving tens of applications for the sharing of such data at a particular moment. A similar point can be made about the relevant legal expertise. Possessing one or a few individuals that have a high level of knowledge on key member state law is unlikely to be sufficient in a context in which a HDAB is receiving a high volume of requests from various Member States throughout Europe. It is submitted that this added dimension of 'quantity' renders the task of HDABs even more problematic. It must also be remembered that HDABs will be largely dependent on state funding (though they may also charge some income also from data access permit requests).[87] This will limit the resources available for recruitment and the payment of salaries. Given that many of the types of expertise outlined here will also be highly in demand within the private sector, HDABs may also face problems of competitivity in terms of being able to attract the necessary talent in the first place.

7.2 The Risk of Developing a 'Rubber Stamp/Tick Box Culture' Process?

These forgoing analysis shows HDABs will have to be extremely well resourced if they are to be capable of carrying out their functions correctly. Indeed the EHDS itself states that Member States must adequately resource HDABs so that they can perform their function properly, stating:[88]

> "Each health data access body should be provided with the financial, technical and human resources, premises and infrastructure necessary for the effective performance of its tasks, including those related to cooperation with other health data access bodies throughout the Union. The members of the governance and decision-making bodies of health data access bodies and their staff should have the necessary qualifications, experience and skills."

The regulation does not however foresee any specific enforcement mechanism for instances where Member States fail to fund HDABs adequately. Given this, the EU Commission will have to fall back on the standard mechanisms for challenging non-compliance with EU law. Whilst there is therefore a theoretical possibility of taking legal action against Member States that under resource HDABs, it is not a simple or readily available option.[89] Although political pressure also presents an important option, it is unclear to what extent pressure in an area that may be considered obscure to those involved in politici debates at the national level might weigh upon the necessary decision makers. Given this, and a context where all states have finite resources, the risks that at least some Member States will not adequately resources HDABs clearly exists.

The author of this paper would suggest however that, given the range of demands outlined in this paper, that even were such bodies to be well resourced (i.e. to a realistic but not utopian level) it would be difficult for them to comply with the range of complex assessments that they seem obliged to perform. Given this, there is a very real risk that the type of compliance that is foreseen within the EHDS will be reduced to cursory checks, for example ensuring that applicants for a data access permit have themselves provided evidence of compliance. This could involve simple checks to see that the applicant has themselves indicated a legal base and provided an explanation for why principles such as data minimization and purpose limitation have been met. In a worst-case scenario such checks could be limited to ensuring that supporting documents have been uploaded and relevant responses (e.g. to an online questionnaire) have been filled in. Falling back on a more superficial level of scrutiny may indeed seem appealing to under resourced HDABs, especially as they could seek to argue that the fact that the GDPR and its requirements still apply to data recipients means

87. Article 62(3) of the regulation states that "Any fees charged to health data users pursuant to this Article shall be transparent and non-discriminatory"

88. Recital 64 of the EHDS regulation

89. For more on the general enforcement options available under EU law see: András Jakab and Dimitry Kochenov, *The Enforcement of EU Law and Values: Ensuring Member States' Compliance* (Oxford University Press, 2017).

that there would be an important level of secondary protection available in addition to their checks (i.e. in the form of enforcement by data protection national supervisory bodies).[90]

It is argued however that such a mindset should be strongly avoided. The innate sensitivity of health data, both in terms of risks at the individual and societal level warrants a more thorough approach. Were such a 'rubber stamp' situation to arise, the risk of such harms occurring would be serious, and perhaps over time inevitable. Such harms are not only intrinsically harmful for both individuals and society but would also lead to an erosion of trust in terms of the willingness of individuals to share their health data. This could have serous long term effects in terms of healthcare avoidance or a reduced body of health data available for scientific research.

In order to reduce such risks, the author of this paper would argue that one possibility is to interpret the EHDS regulation in a way that would provide HDABs with a more realistic set of tasks. In doing so two types of responsibility could potentially be interpreted in such a way as to attenuate the complexity required. The *first* concerns the requirement to check compliance (in terms of a legal base) with relevant national law. The *second* concerns the need to verify whether applicants have been through an ethical review process in a manner that iscompliant with whichever national law is applicable. Both of these requirements are extremely intensive and require a level of knowledge of highly divergent frameworks across Europe that is arguably not feasible. HDABs could for example still check that proposed processing operations were broadly compliant with one of the legal bases within the GDPR but not have to scrutinize national law also. In place of a strict interpretation of the requirements contained within the regulation, HDABs could rather simply ask for applicants to provide evidence of how their proposed data processing is compliant with national law and also how they have complied with any relevant requirements for ethical review.

Not interpreting the regulation as requiring HDABS to scrutinize in detail themselves the relevant national rules in these areas would, it is suggested, reduce the workload per dossier to a more realistic level. It would also leave more space to focus on the key contextual elements of each dossier, considering their domain and background. This would allow HDABs to focus on determinations of substantive issues that vary less between Member States. It is argued that doing so would render tasks such as determining what is adequate in terms of minimization and purpose limitation more feasible, allowing HDABs to perform a meaningful level of analysis. The author of this paper admits that there is a certain paradoxicality to such a proposal. Essentially it entails making part of the assessment conducted by HBADs a 'rubber-stamping' exercise, something that in general is not desirable. It is submitted however that allowing this to occur in some limited areas is the price needed to ensure that it does not happen everywhere.

8. Conclusion

Health Data Access Bodies will play a pivotal role under the European Health Data Space. This paper has focused on their role as assessor of data access permit requests for the use of secondary electronic health data. In doing so it has taken into account three factors that may be useful in indicating to what extent HDABs are likely to be overburdened or not. These are the requirements imposed on the HDABs by the regulation itself, the second is the heterogeneity in terms of data and context HDABs are likely to face (both in terms of data and Member State legal system). The third is the need to potentially respond to many requests and within a limited timeframe.

Requests to HDABs can be made by various entities that want access to electronic health data for secondary processing purposes. The EHDS regulation tasks HDABs with assessing a number or important factors before agreeing to grant a data access permit. This includes *inter alia* that applicants have a valid legal base, that data protection principles such as minimization and purpose limitation are respected. Applicants should also demonstrate that they have complied with any relevant national rules on ethical review and

90. It should be noted that concerns have frequently been raised about the resourcing national data protection authorities also and their consequent ability to perform their tasks properly. See for example: Inge Graef and Jens Prüfer, 'Governance of Data Sharing: A Law & Economics Proposal', *Research Policy*, 50.9 (2021), 104330 https://doi.org/10.1016/j.respol.2021.104330.

oversight.As this article discussed, all of these requirements are extremely complex and require a high level of complex multi-disciplinary expertise. This paper has set out why it is arguably not feasible to expect HDABs to perform their role in this regard as envisaged in the EHDS proposal.

In terms of legal base for example, the EHDS regulation seemingly expects HDABs to enquire about requirements in national law. Whilst this may appear logical given that the GDPR makes clear that some of its legal bases can only be used alongside complimentary national law, the reality of this requirement is that HDABs will have to makedeterminations of this situation not only in the Member State in which they are vested but also potentially any other Member State from where a request might come. Given the hetrogeneity that exists, this is in reality an extremely heavy requirement, both in terms of the expertise it would require and also the time needed to verify claims of compliance with national law. The same is true for the apparent requirement to ascertain that potential data recipients have complied with relevant national rules on ethical oversight. Again, the heterogeneity of the picture not only across European Member States but potentially within them is enormous.

HDABs must combine such enquires with other determinations that are key to ensuring that electronic health data is only shared in a responsible way. This includes adherence to the general principles outlined in articles 53 and 54 for when data should and should not be shared, and adherence to key data protection principles such as data minimization, purpose limitation and the need to anonymize data (where it is possible to do so). As this paper has discussed, these are complex requirements, especially given that in order to make such determinations, it is not only necessary to take into account the domain in which the particular instance of proposed processing exists (e.g. a particular discipline of scientific research) but also the context of each particular project and the nature of the data involved.

As the author of this paper has discussed, given the need to consider potentially many dossiers, from across the EU and within a period of 3 months, it might not be considered realistic for HDABs to perform such a complex range of analysis at both the speed and scale required and, in an ongoing fashion. It seems likely that HDABs will face competition for resources with other state funded entities. HDABs will also be competing with the private sector to recruit the types of highly experienced personnel that will be needed to perform the types of analyses outlined in this paper.This makes it unlikely that HDABs will be able to secure the necessary personnel to complete the types of assessment at the scale that appears to be envisaged in the EHDS regulation. The author of this paper would therefore argue that there is a serious risk that HDABs are forced by pragmatic constraints in such circumstances to perform a ‘rubber-stamp’ exercise whereby they are merely able to ascertain that data access permit requests have provided reasons for why such conditions have been met. In such scenarios HDABs would lack the means to scrutinize such reasoning deeply and would have to accept it at face value.

In order to avoid this risk it has been argued in this paper that it is necessary to be more realistic about the different determinations that HDABs are obliged to make when deciding upon whether or not to grant a data access permit. Given the inherent complexity involved it has been suggested that some of the requirements upon HDABs could be interpreted in a loose manner so as to allow others to receive the level of attention they deserve.This includes the need to ensure that national rules concerning the use of legal bases for the processing of data are complied with. Whilst adherence to such rules is essential, it is suggested for pragmatic reasons that HDABs do not need to analyse such compliance themselves too intensively. Given that adherence with such national law requirements is currently required under the GDPR it is suggested ensuring compliance in this area can be left with pre-existing mechanisms (e.g. under national supervisory authority supervision). Such mechanisms not only already exist, but are also staffed by individuals with a correct knowledge of national law.Similar arguments could made concerning the requirement of HDABs – to ensure that national rules on ethical oversight are complied with. Ensuring compliance with such a diverse and asymmetrical web of requirements will arguably require a disproportionate commitment of resources in an area where there should, in theory, be mechanisms in place at the national, regional and institutional levels to ensure compliance. In these areas, and to reduce the workload to more realistic levels this paper has suggested that HDABs could merely seek to ensure that potential data recipients provide adequate evidence that such requirements have been complied with.

Interpreting these requirements in a liberal manner, is not without concern. Doing so however recognizes that HDABs will exist in a world where demand may be high and resources finite. Given this it better for such bodies to focus their analytic energy on a smaller set of core requirements, *inter alia* on determining what the requirements of data minimization, storage limitation and the need for anonymization (where possible) mean in particular contexts. Such requirements themselves will be extremely demanding, especially given the sheer variety of differing contextual backgrounds and types of data they must be assessed against. Such assessments will however at their core concern similar parameters, that should allow expertise to be both better pooled and more focused. It is regrettable that such a proposal would turn some of the assessment that HDABs must make into a form of 'rubber-stamping' or 'tick box' exercise, but it is argued that this is a necessary and pragmatic price that is worth paying to ensure that the whole process does not turn out this way.

[w]