Universiteit
Leiden
The Netherlands

A fair balance: health data protection and the promotion of health data use for clinical and research purposes

Kist, I.R.

Citation
Kist, I. R. (2024, June 5). *A fair balance: health data protection and the promotion of health data use for clinical and research purposes*. Retrieved from https://hdl.handle.net/1887/3759726

Version:	Publisher's Version
License:	Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden
Downloaded from:	https://hdl.handle.net/1887/3759726

Note: To cite this publication please use the final published version (if applicable).

Conclusions, recommendations and final considerations for future research

7. Conclusions, recommendations and final considerations for future research

This thesis was prompted by the problematic exchange of health data, both within the Netherlands and beyond. At least four issues are at the root of this, i.e.:[499]

a) the diverse interpretations of essential elements of consent;
b) the use of various legal bases within the European Union for the processing of health data;
c) the mere focus on protecting individual rights and interests while obstructing the free flow of data and, hence, the societal interest;
d) the shift away from a risk-based approach towards rule-based regulatory compliance.

Therefore, I aimed at answering the following main research question:

> *In what way can a balanced approach be found for the exchange of health data that serves the data protection of the individual and patient on one hand, and the furtherance of health research in the interest of society, on the other?*

This chapter starts with an answer to the main research question (section 7.1). Then, seven recommendations are shared (section 7.2). This chapter ends with six final considerations for further research (section 7.3).

[499] Chapter 1: Introduction.

7.1. Answering the main research question

The short answers to the main research question are as follows. A balanced approach can be found in the following four ways. Firstly, a broader interpretation of the concept of consent is possible to facilitate secondary health research in the Netherlands and the European Union. Although consent is an autonomous concept of EU law, which must be interpreted uniformly throughout the EU, member states interpret and implement the legal ground of consent in various ways. This obstructs the use of health data for secondary research purposes.

In the Netherlands, the lawful basis of consent is used following the provisions in the GDPR and UAVG.[500] Furthermore, the WGBO contains conditions for the further use of health data by others than the health care provider.[501] The GDPR provides for explicit consent as an exemption to the prohibition of the processing of health data. Recital 33 GDPR allows for some granularity of consent for research purposes.[502] Though the EDPB considers that the granularity should not be stretched too far, it does not further clarify what could fall within this broader scope.[503] In sum, a first answer is that the lawful basis of consent could be used for secondary health research provided that the granularity of consent is further explicated.

Secondly, the use of other lawful bases besides consent can be a solution in the Netherlands and the European Union for the legitimation of secondary health research.[504] The lawful bases of the public interest[505] as well as the legitimate interests[506] are used in the European Union.[507] A separate legal ground for secondary research purposes has not been included in the GDPR and could be a solution to resolve the issue of

[500] Article 6 (1) (a) together with article 9 (2) (a) and article 89 (1) GDPR; article 22 together with 24 UAVG.
[501] Article 7:457 and 7:458 WGBO.
[502] Recital 33 GDPR: *"(…) Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognized ethical standards for scientific research (…)."*
[503] EDPB, Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research, 2 February 2021, para 26, at 7:
"(…) [T]he EDPB points out that, as stated in the EDPB Guidelines 05/2020 on consent under regulation 2016/679 (§153 and following), even though, for the cases where purposes for data processing within a scientific research project cannot be specified at the outset, Recital 33 allows as an exception that the purpose may be described at a more general level, the GDPR cannot be interpreted to allow for a controller to navigate around the key principle of specifying purposes for which consent of the data subject is asked. Therefore, when research purposes cannot be fully specified, a controller must seek other ways to ensure the essence of the consent requirements are served best, for example, to allow data subjects to consent for a research purpose in more general terms and for specific stages of a research project that are already known to take place at the outset."
R. Becker et al., Secondary Use of Personal Health Data: When Is It "Further Processing" Under the GDPR, and What Are the Implications for Data Controllers? *European Journal of Health Law*, 29, 1-29. https://doi.org/10.1163/15718093-bja10094.
[504] Chapters 3 and 4, in particular sections 3.2.2, 3.3, 3.3.2, 3.5, 4.3 and 4.5.
[505] Article 6 (1) (e) together with article 9 (2) (j) and article 89 (1) GDPR.
[506] Article 6 (1) (f) GDPR.
[507] European Commission, Assessment of the EU Member States' rules on health data in the light of GDPR, including the Annex with country fiches of all EU MS. Specific Contract No SC 2019 70 02 in the context of the Single Framework Contract Chafea/2018/Health/03. Also, E.B. van Veen, R.A. Verheij, Further use of data and tissue for a learning health system: the rules and procedures in The Netherlands, compared to Denmark, England, Finland, France and Germany, MLCF/Nivel, Utrecht, May 2022.

a proper lawful basis for secondary health research purposes.[508] Additionally, with the developments of the EHDS, provisions have been included as regards the use of data for healthcare and research purposes, referred to in the EHDS as the primary and secondary use.[509] For efficient data sharing among member states, it is desired that the member states allow for the use of different lawful bases for the exchange of health data for research purposes.[510] In the Netherlands, an amendment of article 24 UAVG, as well as articles 7:457 and 7:458 WGBO would be needed if the EHDS is adopted with the provisions on the secondary use of data.[511] This would also require an amendment of the draft Wzl. In sum, a second answer is that lawful bases other than consent legitimize the use of health data for secondary research purposes. Mutual recognition by the member states is a key factor in the use of different legal grounds for secondary research purposes. An amendment in the Dutch legislation is needed as regards the secondary use of data if the EHDS is adopted.

Thirdly, a balance can be found in the individual's autonomy and (informational) self-determination vis-à-vis the accountability of the health institution that processes his data, and the attention drawn to the free flow of data.[512] In health care and research, the individual exercises control over his data with the expression of his consent. However, he may not always be able to oversee the consequences of the expression of his will. In health care, a balance can be found in the triangle of care with the involvement of the care provider, the formal or informal representative and the care receiver when the individual is not or no longer capable of expressing his consent.[513] In health research, the balance can be found in the acknowledgement that the GDPR does not have as its objective

> *"(…) [t]o grant data subjects control over their personal data as a right in itself, or that data subjects must have the greatest control possible over those data."*[514]

[508] As explored in the United Kingdom in the proposals to the revision of the UK GDPR. See Chapter 5 supra.
[509] European Commission. (2022d, May 3). Proposal for a Regulation of the European Parliament and of the Council of 3 May 2022 on the European Health Data Space (Text with EEA relevance), articles 2 (2) (d) and (e).
Also, European Data Protection Board, Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research, 2 February 2021, para 18, at 6.
[510] EDPB, 2 February 2021, footnote 509, para 16, at 6:
"It is advisable that controllers should as far as possible make an effort to limit the consequences of different Member States' legal regimes for processing health data for scientific research purposes, for instance by optimizing and thus harmonizing the rights of data subjects irrespective of the Member State they live in."
[511] Veenbrink, J. M., van de Gronden, J. W., & Glas, L. R. (2022). *Juridisch Advies over het voorstel voor een Verordening betreffende de Europese ruimte voor gezondheidsgegevens (European Health Data Space)*, 58.
[512] Hooghiemstra, T. (2018). *Informationele zelfbeschikking in de zorg*. SDU.
[513] Chapter 2, in particular sections 2.4 and 2.5.
[514] UI v Österreichische Post, Opinion of Advocate General Campos Sánchez-Bordona (Court of Justice of the European Union, 2022). ECLI ECLI:EU:C:2022:756, paras 73 – 74.

Furthermore, the GDPR aims at protecting individual rights together with the free flow of data.[515] Thus, a third answer is to find the balance between the individual's autonomy and self-determination vis-à-vis the free flow of data. The triangle of care, with the involvement of the individual, the care provider and the formal or informal representative may be a solution in health care when the individual is unable to express his will about his health and the necessary care for him. In health research, the accountability of the health institution is shown with the technical and organizational measures taken.[516] Furthermore, with the use of other lawful bases than consent, the focus is shifted from the individual's consent towards the public or legitimate interests of the data controller.[517] Additionally, the GDPR itself provides for the balance between the data protection rights on the one hand, and the free flow of data, on the other.[518]

Fourthly, a balance can be found in a risk-based rather than a rule-based approach by supervisory authorities.[519] To this end, clarification is required as regards the roles of the supervisory authorities. In Dutch health care and research, both general and sectoral supervisory authorities monitor compliance with general data protection legislation (GDPR, UAVG) and sectoral health legislation (inter alia, proposal for a regulation on the EHDS, WGBO, draft Wzl, Wlz). In Europe, with the development of the EHDS, yet another supervisory mechanism is established, the Health Data Access Bodies.[520] The relationship between the European and Dutch supervisory authorities, as well as between the Dutch authorities, deserves clarification as to the respective roles, tasks and functions. Furthermore, the data controller has to show compliance with, inter alia, data protection impact assessments,[521] records of processing activities[522] and data breaches.[523] A balance can be found in the development of best practices for fair, transparent, and lawful data processing by the data controllers and, hence, a more risk-based approach by the supervisory authorities. Thus, a fourth answer is that monitoring authorities could focus on risk-based rather than rule-based

[515] Article 1 (1) GDPR: *"This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data."*
[516] Article 24 (1) and (2) together with article 32 (1) GDPR.
[517] For instance article 6 (1) (e) GDPR: *"(…) [P]rocessing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller"*, or article 6 (1) (f) GDPR: *"(…) [P]rocessing is necessary for the purposes of the legitimate interests pursued by the controller (…)."*
[518] Recital 4 GDPR: *"The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality (…)."* And, Recital 6 GDPR: *"(…) Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organizations, while ensuring a high level of the protection of personal data (…)."*
[519] Section 5.3.3 supra.
[520] Article 37 EHDS. See section 6.4.2 supra.
[521] Article 35 GDPR.
[522] Article 30 GDPR.
[523] Article 33 (5) GDPR.

monitoring. Furthermore, the different roles, tasks and functions of these supervisory authorities should be clarified.

The following sections contain a more detailed answer to the main research question with a focus on the following components. I start with the legal framework (section 7.1.1) upon which I continue with the legitimation for the use of health data (section 7.1.2). Then, I focus on the individual rights on the one hand and the free flow of data on the other (section 7.1.3). Lastly, I reach conclusions on monitoring compliance (section 7.1.4).

7.1.1. The legal framework

A balanced approach can be found in the GDPR itself. The GDPR provides for a general legal framework and does not prescribe a particular interpretation. Then, new developments take place with the proposal for a Regulation on the European Health Data Space. This Regulation aims at promoting the exchange of and access to different types of electronic health data, including electronic health records, genomics data, patient registries to further health care and research.[524] Additionally, the Data Act and Data Governance Act have entered into force since the start of this thesis.

In the Netherlands, the Dutch Act on Quality Registrations (*Wet Kwaliteitsregistraties Zorg*) is currently prepared. In the field of research, the draft Dutch Authority over Human tissue Act (*Wet zeggenschap lichaamsmateriaal, Wzl*) is prepared and a renewed proposal for an amendment is foreseen in the spring of 2024. In view of most recent developments of the EHDS and the lawful basis of processing for secondary use, the plenary debate was postponed in 2023. If the EHDS is adopted, then article 24 UAVG, as well as articles 7:457 and 7:458 WGBO would need to be amended. Lastly, the initiatives by the executive power, i.e., the Dutch Ministry of Public Health, Welfare, and Sport, in cooperation with representatives from the field who joined their efforts in Health-RI and the Royal Netherlands Standardization Institute (*Nederlands Normalisatie Instituut, NEN*), have presented the first results.[525]

7.1.2. The legitimation for the use of health data

A balanced approach to the legitimation for the use of health data serves to enhance the exchange of data for clinical and research purposes. The legitimation with the lawful basis of consent for the use of health data for clinical and research purposes is not always adequate for the following reasons. Firstly, the four elements of consent cannot always be satisfied.[526] Secondly, a comprehensive interpretation of consent among EU

[524] Explanatory memorandum EHDS: *"(…) [T]he uneven implementation and interpretation of the GDPR by Member States creates considerable legal uncertainties, resulting in barriers to secondary use of electronic health data."*
[525] https://www.health-ri.nl/lees-en-kijk-materiaal. Accessed 29 January 2024.
[526] Article 4 (10) GDPR.

member states is absent, as the meaning and scope of consent differ in the Union. Thirdly, the percentage of consent given among particular diseases, populations, and minority groups, for instance, differs. As a result, a biased research population may exist. Fourthly, the individual is not always capable to express his will with consent.

Furthermore, the individual's consent does not exempt the controller from implementing appropriate safeguards for the data processing. Each data processing must be carried out in accord with the general data protection principles of article 5 GDPR. In short, the controller is responsible for safeguarding these principles. The processing must take place based on a lawful basis. Additionally, the individual's rights must be respected. Again, regardless of which lawful basis is used, the controller must fulfill these obligations. Thus, the focus should not be primarily on determining the proper legal basis for the data processing, but rather on the underlying assessment and guarantee that the data controller respects legal principles and human values.

In some member states of the European Union, recourse can be had to another lawful basis, such as the public interest or legitimate interests.[527] In the United Kingdom, a separate lawful basis for (health) research is considered.[528] The developments of the EHDS are of particular importance, as well as the recent developments in the Netherlands.[529] These recent developments in the Netherlands are promising with a new amendment to the proposal of the Wzl and the advice from the Dutch Data Protection Authority on the excess mortality rates during the COVID-19 pandemic.[530] If the Dutch proposal of the Wzl will be amended in view of the EHDS, then articles 7:457 and 7:458 WGBO, as well as article 24 UAVG, would need to be amended as well. In the course of time, integral sectoral health legislation in the Netherlands is an option for establishing a separate lawful basis for secondary health research.

As regards the further processing for research purposes, the data controller, i.e. the health institution in this thesis, must demonstrate that the processing is based on a lawful basis.[531] The controller must show compliance with the principles enshrined in article 5 GDPR, and must adopt the institutional and technical safeguards.[532] Thus, the special regime regarding the further processing for research purposes may not constitute a derogation from the data subject's rights.

[527] Article 6 (1) (e) together with article 9 (2) (i) or (j) and article 89 (1); article 6 (1) (f) together with article 89 (1) GDPR.
[528] Chapter 5 supra.
[529] Section 7.1.1 supra. A Letter to Parliament is expected in the spring of 2024 in the Netherlands. This letter will address, inter alia, data sharing in the interest of secondary research purposes.
[530] Autoriteit Persoonsgegevens, Adviesverzoek onderzoek oversterfte, 13 februari 2023. https://www.autoriteitpersoonsgegevens.nl/uploads/imported/advies_ap_onderzoek_oversterfte.pdf. And, https://www.eerstekamer.nl/behandeling/20230223/brief_regering_verzoek_uitstel/document3/f=/vm11ejjmm2sk.pdf. Accessed 29 January 2024.
[531] Article 6 and 9 together with article 89 (1) GDPR.
[532] Article 24, 32 and 89 (1) GDPR. European Data Protection Supervisor, A Preliminary Opinion on data protection and scientific research, 6 January 2020, 17.

7.1.3. Individual rights or interests and the free flow of data

The rights to data protection and privacy are not absolute. These rights must be seen in conjunction with the free flow of data and the protection of other human rights or interests. The general framework of the GDPR leaves room for a comprehensive interpretation of concepts. Furthermore, the individual rights or interests are not guaranteed only by the lawful basis of consent. Other lawful bases must equally safeguard these rights and interests. Moreover, regardless of which lawful basis is used, the controller must fulfill its obligations in chapter III GDPR on the rights of the data subject.

Additionally, the individual's rights must be safeguarded in today's innovative developments and the new position that the individual plays in monitoring his own health. The traditional relationship between the care provider and care receiver is absent.[533] The EHDS may provide additional safeguards. This act focuses on data protection on the one hand and the necessity of and the challenges to the exchange of data for health care, research, and innovations on the other. Innovative developments are already taking place and require innovative answers to both the individual and his data.

A comprehensive interpretation of the concepts is both legally possible and necessary in the search for a balanced approach between data protection and the free flow of data. Concepts in the law are interpreted differently among member states and within the member states themselves. The concepts need not only be interpreted from the perspective of individual self-determination, autonomy, and the rights or interests of the individual, but also from the perspective of the free flow of data and the furtherance of health research. Thus, data processing of health data for care and research purposes is in the best interest *of* a specific patient, and in the societal interests *for* all patients.

7.1.4. Monitoring compliance

Lastly, a balanced approach is required to monitoring compliance by the Data Protection Authority and other (sectoral) supervisory mechanisms. This requires a risk-based approach from the authorities to serve both the individual rights or interests and the free flow of data. One of the main principles in the GDPR concerns the accountability of the controller.[534] However, a rule-based system of regulatory compliance rather than a risk-based system has been established.

The data controllers must demonstrate compliance with, for instance, a record of data processing activities (article 30 GDPR) and data protection impact assessments (article

[533] Chapter 6 supra.
[534] Article 5 GDPR.

35 GDPR). Additionally, prior consultation with the supervisory authority must take place where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk (article 36 GDPR). The appointment of a data protection officer must be notified as well (articles 37 – 39 GDPR). Furthermore, the controller is obliged to notify the Data Protection Authority of all data breaches unless a breach does not pose a material risk to the rights and freedoms of the individual (articles 33 and 34 GDPR). These requirements place a burden on both the organizations and the individuals, since time is devoted to compliance rather than to the development of best practices for fair, transparent, and lawful data processing.

With the new legislative developments of the EHDS and AI Act, questions are raised by the EDPB and EDPS on the interaction between (additional) supervisory bodies established within the EHDS and AI Act and the existing supervisory bodies established by the GDPR and national, sectoral health legislation.[535] In the Netherlands, the Dutch Health care Inspectorate (*Inspectie Gezondheidszorg, IGJ*) and the Dutch Health care Authority (*Nederlandse Zorgautoriteit, NZA*) monitor health care. The Dutch Data Protection Authority provides advice and carries out supervision of data protection.

Overall, a wide array of supervisory and monitoring mechanisms have been established in the applicable legislation and are forecast to be established with the future legislative development of the EHDS. The EHDS proposes a governance structure aiming at closer cooperation between national data protection authorities and sectoral health bodies. In the Netherlands, the Dutch Ministry of Public Health, Welfare and Sport launched the Program HDAB-NL on 23 December 2023.[536] Clarification about the different roles, tasks and functions is needed in such a manner that the health care and research institutions know what is expected and which authority they can consult for further questions.

7.2. Recommendations

In the context of this thesis, I offer the following seven recommendations to the European and Dutch legislature, as well as to the supervisory authorities in data protection and health law.

[535] EDPB - EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021. Also, EDPB - EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space, 12 July 2022.

[536] https://www.gegevensuitwisselingindezorg.nl/actueel/nieuws/2023/12/04/vws-start-programma-health-data-access-body-hdab-nl. Accessed 29 January 2024.

Recommendation 1: Emphasize the burden of control by the data controller

Firstly, I recommend that the data controller acknowledges and emphasizes its burden of control as regards data processing. The individual is neither able to exercise sufficient control over the processing of his data, nor is he able to implement the necessary technical and organizational measures. Therefore, regardless of which lawful basis is used for data processing in health care and research, the data controller must take the necessary technical and organizational measures. It must meet the principles of fairness, necessity, and proportionality, as well as data quality (recitals 32, 33, 42, and 43, article 5 GDPR). In addition, the controller must be able to demonstrate that consent is given (recital 42, articles 4 (11) and 7 GDPR). Furthermore, the data controller must inform the individual in a clear, transparent manner about the data processing. The information provided to the individual must be comprehensible and easily accessible, for instance on the internet, via information leaflets or video-screens at the data controller's premises. The individual should not carry the weight of his consent as a legitimation for the processing of his health data. The controller is accountable for the data processing regardless of the lawful basis applied.

Recommendation 2: Mutually agree on the use of various lawful bases for secondary research purposes

Secondly, I recommend that a further analysis be carried out whereby other lawful bases, in addition to consent, serve as a proper legitimation for the secondary use of health data in research, and under which conditions these lawful bases can be applied. In the European Union, other lawful bases than consent are used by member states that may serve as potential solutions in the Netherlands as well. A coherent European approach has not yet been achieved, as the GDPR allows member states to adopt various and diverging implementation laws. Nevertheless, the fact that the processing of health data for research across Europe is carried out pursuant to different perceptions of consent, as well as other legal bases, does not necessarily mean that the individual's rights receive better protection in country X than in country Y. Yet, these differences complicate trans-border data flows between the EU and elsewhere.

I recommend that member states acknowledge the use of different legal grounds based on which the data exchange for health research takes place. This requires mutual trust between the research institutions that the rights and interests of the individual are safeguarded, while the controller undertakes the necessary technical and organizational measures, regardless of which lawful basis is applied. It also requires mutual trust between the member states as regards the choice of a lawful basis and specific member state laws. Some member states have specified, prescribed, or excluded the

lawful bases for processing health data for scientific research in specific member state law. Other member states have explicated in member state law whether an exemption on article 9 (1) may be based on article 9 (2) (g), (i) or (j) in conjunction with article 6 (1) (a), (e), or (f) GDPR. Since a European Code of Conduct does not seem feasible in the short run, I recommend that the potential lack of homogeneity among member states be solved with the mutual acknowledgement of different lawful bases used for the secondary use of health data for research. Furthermore, the developments in the EHDS should be aligned with the current legal framework of the GDPR, AI Act, Data Act and Data Governance Act.

Recommendation 3: Aim for a comprehensive interpretation of the lawful basis of consent

Thirdly, I recommend that the lawful basis of consent be interpreted in a comprehensive manner. Suffice it to say that the elements of consent, i.e., the freely given, explicit, informed, and unambiguous consent, require an interpretation that coincides with reality and cultural differences.

In health care, I recommend that careful attention be given to the capacity of the individual and, therefore, the expression of his consent. With his consent, the individual expresses his free choice and self-management in the care given to him. However, he may withhold himself from required care when he expresses his will, for instance in the case of individuals developing dementia. In these situations, the triangle of care with the involvement of the individual, health provider, and representative deserves further attention. In practice, this not only requires a legislative amendment, but also a procedural and system change since the access to the electronic health record takes place with the individual's consent himself. A formal or informal representative may request authorization to access his health record but again, consent from the individual himself must be given. Then, the vicious circle of consent is complete.

In the case of health research, the element "informed" may not be completely achieved when the research was initiated. The researcher may not be aware of findings that become known at a later stage and that may form the basis for new research. Asking repetitive consent may place a burden on the individual, particularly in the case of longitudinal studies, which can last for several decades. The individual's consent is also reflected in the trust and the reasonable expectations based on his relationship with the controller, i.e., the health research institution.[537]

[537] Recital 50 GDPR.

Recommendation 4: Separate the lawful basis of consent from the assumption of the individual's full control over his data

Fourthly, I recommend that a fair balance be achieved in practice between data protection rights and the free flow of data. To this end, I recommend that the lawful basis of consent be separated from the assumption that the individual has full control over his personal data. The individual, in his role as patient or client who receives medical care and whose data could be of value for health research, may very well not read, let alone understand privacy statements or balance the pros and cons of his consent. The GDPR (articles 12 – 22) grants the individual a number of rights as regards his personal data, rights that he can exercise towards the data controller. However, this does not mean that he actually owns or controls the data himself or that the GDPR grants the individual full control over his data.

Recommendation 5: Explain concepts in European legislation

Fifthly, I recommend that the concepts of secondary use, further processing, public interest and research in the GDPR be further detailed, preferably by the EDPB. The interpretation of the GDPR framework substantially differs among member states. This has resulted in fragmentation rather than a common approach to the interpretation and use of health data. Additionally, I recommend that similar concepts used in the GDPR, the EHDS, and the AI Act be explained. Confusion arises when there is a different scope or interpretation of similar concepts used in the GDPR, EHDS, and AI Act. These concepts warrant further clarification, also as regards the relationship between the general GDPR and the specific EHDS and AI Act.

As regards the EHDS in particular, I recommend further clarification of the concepts of 'primary use of health data' and 'secondary use of health data', in line with the EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space. For instance, health data from diagnostics and care are used to improve the quality of care and for public registries. The data may also serve as an important source for secondary research. Furthermore, the individual who monitors his own health may also present the data collected from his wearable to the health provider. The question arises when the data are processed for primary use and when they are collected for secondary use. The GDPR does not include the EHDS concept of "secondary use of health data." Instead, it uses the concept of "further processing of personal data." The concept of "further processing" refers to the purpose for which the controller originally processed the data.

Recommendation 6: Aim for a risk-based approach in monitoring and supervision

Sixthly, I recommend that the risk-based approach, which has been included in the GDPR, be given new impetus by the supervisory authorities. In practice, data controllers have to demonstrate compliance with the obligation to record data processing activities (article 30 GDPR), Data Protection Impact Assessments (article 35 GDPR) and to record data breaches (article 33 (5) GDPR). Furthermore, the presence of a data protection officer is required (articles 37 – 39 GDPR). Although the obligations have proved useful, they do not ensure that the individual rights or interests are guaranteed. I recommend that the data controller focus more on the balance between the individual rights or interests and the free flow of data, while fulfilling the obligations enunciated in article 5 GDPR. The return to a risk-based approach by the data controller also requires a shift by the data protection authorities.

Recommendation 7: Aim for a closer cooperation between Data Protection Authorities and sectoral supervisory mechanisms

Seventhly, I recommend that the Data Protection Authorities in the Netherlands and the European Union cooperate more closely with sectoral, health care supervisory bodies. This way, the individual is protected from both the data protection and health law perspectives. Since the individual plays an active role in monitoring his own health and sharing data beyond the traditional care provider–care receiver context, I recommend that the governance structure be extended to safeguard his position in both contexts. The governance structure offered by the EHDS can be a starting point to closing the gaps in the individual's data protection rights regarding health beyond his role as a patient in the traditional setting. In addition, the EHDS can also provide a framework to close the gap between the supervisory mechanisms in health and the general data protection authorities.

7.3. Final considerations for future research

Although I identified a considerable number of pending questions while working at the Netherlands Cancer Institute – Antoni van Leeuwenhoek hospital, questions that comprise a valuable basis for my thesis, I have not been able to connect all the capillaries. In delineating my thesis, I purposely left open a number of questions that would benefit from further research. Therefore, I end this study with six final considerations for future research.

Firstly, future research is recommended on the principles of solidarity and reciprocity in secondary health research.[538] The starting point for this research could be the Universal Declaration of Human Rights (UDHS), which was adopted by the General Assembly of the United Nations in 1948, where article 27 (1) states that

> *"Everyone has the right (…) to share in scientific advancement and its benefits (…)."*

Furthermore, the GDPR seeks to harmonize the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data among member states. In health research, personal data, either directly or indirectly identifiable to the individual, are of crucial importance to advancing science. Today's patients and their data form the basis of tomorrow's research. Their data sharing may not cure those patients, but may cure those of future generations indeed.

Research could be carried out to determine how the individual may, could or perhaps should serve the common good in sharing his personal data for secondary health research. Data processing of health data for care and research purposes is in the best interest *of* a specific patient, and in the societal interests *for* all patients. The other side of the same coin comprises the limits to economic gain with these personal health data. Data registers of health data and biobanks are valuable sources for investors and, therefore, a driving force behind the global health data economy. Further research could analyze the limits to the individual solidarity and reciprocity as regards data sharing in health.

In a broader perspective, such further research fits into the debate on how privacy and data protection should be regulated, particularly as regards the discrepancy between the so-called Individual Control Model and the Societal Structure Model. The Individual Control Model aims

> *"(…) to empower individuals with rights to help them control the collection, use, and disclosure of their data.*[539]

The Societal Structure Model starts

[538] B. Prainsack, (2018). The "we" in the "me" solidarity and health care in the era of personalized medicine. *Science, Technology, & Human Values*, 43(1), 21-44. R. Yotova, & B.M. Knoppers, (2020). The right to benefit from science and its implications for genomic data sharing. *European Journal of International Law*, 31(2), 665-691.

[539] D.J. Solove & W. Hartzog (2024). Kafka in the Age of AI and the Futility of Privacy as Control (January 5, 2024). *104 Boston University Law Review* (2024, Forthcoming), at 2. Available at SSRN: https://ssrn.com/abstract=4685553 or http://dx.doi.org/10.2139/ssrn.4685553. Accessed 11 February 2024.

> *"(…) [w]ith the recognition that privacy is not purely (or even primarily) an individual interest; instead, privacy should be protected for the purpose of promoting societal values such as democracy, freedom, creativity, health, and intellectual and emotional flourishing."* [540]

Furthermore, the Individual Control Model presupposes the individual control over their data, whilst the individual cannot completely control his data, especially in today's world where the individual is surrounded by technological innovations:

> *"Turning to modern digital technologies, individual control is often an illusion. People don't exercise control in a meaningful way. Merely being in a command center with various switches, buttons, and levers is mere theater unless people have the ability and knowledge to operate the controls. The individual's ability to exercise control always exists within a larger power structure."* [541]

Secondly, future research is recommended into the elements of informed (ethical) consent as enunciated in the Clinical Trials Regulation, and the elements of consent in the GDPR, especially with regard to new legislative developments in the Netherlands. For instance, the draft Wzl has incorporated the four elements of consent from the GDPR. Research could be carried out to determine when informed (ethical) consent or when GDPR consent is privileged to legitimize the use of health data for research purposes. Furthermore, the elements of consent and the way in which this consent is expressed by the patients deserve further attention. Lastly, an alternative legal ground could be considered in the Netherlands, as regards the (further) use of data for scientific research. The EHDS has paved the road for more integration in the field of health at EU level. These developments will influence the legal developments in the Netherlands as well.[542]

Thirdly, future research is recommended on the interaction between latest European legislative initiatives (EHDS, AI Act, Data Act, and Data Governance Act) and the Dutch legislative developments (inter alia, the draft WzL). Additionally, future research is recommended on the interaction between the GDPR, the UAVG, and specific, sectoral health legislation. This future research could also include a further

[540] D.J. Solove & W. Hartzog, footnote 539, at 7.
[541] D.J. Solove & W. Hartzog, footnote 539, at 11.
[542] Organization for Economic Co-operation and Development. (2021). Toward an integrated health information system in the Netherlands. Draft interim brief and recommendations, at 29:
"Revisions may be needed to legacy legislations that are posing unnecessary obstacles to an integrated health information system, such as revisions to the Medical Treatment Contracts Act (Wgbo) to allow for lawful alternatives to consent for data exchange and uses in the public interest; to legislation authorizing the Central Bureau of Statistics to allow it to act as a central hub for access to health datasets; and to regulations related to consumers and markets that prevent health care collaborations and data integration."

elaboration on terminology in the current legislation, as well as and compared to the legislative proposals in the Netherlands and Europe.

Fourthly, future research is recommended on the mission and tasks carried out by data protection authorities and sectoral supervisory bodies. Supervisory authorities have been established in the health sector, both European and national, and both general and specific. In the Netherlands, the Dutch Health care Inspectorate (*Inspectie Gezondheidszorg en Jeugd*, IGJ) and the Dutch Health care Authority (*Nederlandse Zorgautoriteit*, NZA) supervise the health care sector, while the Dutch Data Protection Authority (DPA) supervises data protection in general. Furthermore, the Dutch Data Protection Authority carries out supervision as regards the AI Act as well. A European Health Data Space Board will also be created as regards the re-use of health data, which builds on the framework introduced by the Data Governance Act. This future research could not only unravel the patchwork of monitoring mechanisms in Europe and among member states, but it could also elaborate on the question of how these authorities could design risk-based rather than rule-based regulatory compliance.

Fifthly, future research is recommended regarding the individual's own role in monitoring his health. The processing of health data by commercial service providers may pose a risk to personal data protection. In Chapter 6, my co-author and I analyzed the traditional relationship between the care provider and receiver. This relationship is absent when the individual engages into monitoring his own health whilst buying self-tracking devices. Future research could further unravel the individual autonomy, self-determination and informational privacy amidst the use of new technologies.

Lastly, further research is recommended regarding the proper communication strategy for informing a patient population, a nation's population, or any other population in the EU, about the use of his data for clinical and research purposes. Regardless of which lawful basis is chosen for the legitimation of the exchange of data, the population should be reached in the most efficient way and with the best informative tools. This research should consider cultural influences, different educational backgrounds and literacy of the European citizens. A tailor-made communication strategy for different target groups contributes to a feeling of trust and willingness to share health data.