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

Kist, I.R.

13. Summary

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

Introduction

This thesis was largely conducted during the COVID-19 pandemic, in a world surrounded by technological innovations, where the individual has become an active player in monitoring his own health. This thesis has found a balance between individual data protection rights and the free flow of data. On the one hand, this balance serves to protect the individual and his data. He is entitled to be informed about the use of his data and to invoke his rights as a data subject. On the other hand, health care must be given and health research must be carried out using personal data within and beyond national borders.

The main research question reads as follows:

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

Approach

The legal research methodology applied in this thesis consists of doctrinal legal research. Both primary and secondary sources of the law were scrutinized and case law was included. Proposals for European and Dutch legislation were analyzed as well, such as the European Health Data Space (EHDS). Furthermore, publications and academic research carried out in previous studies were analyzed. This thesis also comprises elements of co-production of knowledge, in close cooperation with the Netherlands Cancer Institute – Antoni van Leeuwenhoek hospital.

Results

This thesis has yielded the following results. Firstly, as regards health care, the lawful basis of consent is not the optimal lawful basis if the individual is not or no longer capable of expressing his will. The strength lies in the triangle of care where both the individual, the care provider and the formal or informal representative play a role to give the individual the best care possible.

Secondly, in today's world with technological innovations, the traditional relationship between the care provider and care receiver may be absent. In existing health law, the care provider acts pursuant to the professional medical secrecy and the health

system is based on the patient's informed consent of shared decision-making. In the new health context, the individual gives his consent to the processing of health data outside the realm of traditional health care. The traditional legal system does not protect him and his personal health data in this new health context. A legislative gap exists in the protection of health data where the individual interacts with organizations that process his data beyond the traditional relationship between care provider and receiver.

Thirdly, as regards secondary health research, Dutch legislation provides for explicit consent as the primary lawful basis. However, the focus solely on consent obstructs scientific health research. The GDPR provides for other lawful bases, such as the public interest and legitimate interests, used in other countries in the European Union. Additionally, the EHDS provides for a legal ground for the primary and secondary use of data. The secondary use also includes secondary health research.

The Dutch Code of Conduct for Health Research provides for a layered structure of consent: explicit, specific consent, general (broad) consent and the exceptions to the lawful basis of consent as included in article 7:458 WGBO and article 24 UAVG. The latter exceptions include a no-objection system and can be used when the conditions of these articles are fulfilled. Revised sectoral health legislation in the Netherlands may eventually solve the issue of the lawful basis for secondary health research.

Fourthly, as regards monitoring by supervisory authorities, risk-based regulatory compliance could facilitate international data sharing. Moreover, risk-based regulatory compliance requires a proactive approach from the organizations to demonstrate accountability and transparency while the burden of demonstrating compliance is reduced at the same time. At the same time, risk-based regulatory compliance also requires a different approach from the data protection authorities that monitor compliance.

Analysis

Though the objective of the GDPR was to provide a set of harmonized data protection laws across all member states, this aim has not yielded full effects in terms of data sharing for health care and research purposes. The GDPR has created a fragmented legal landscape due to legal incongruities in national (implementation and sectoral) legislation, as a result of which cross-border collaboration is obstructed. Several lawful bases are used throughout the European Union for the secondary use of health data for scientific research. Furthermore, provisions in the GDPR leave room for different interpretations and cause delays in collaboration agreements. For instance, there is

some ambiguity in defining concepts such as consent, research, purpose (limitation), and the further processing of personal data.

Specifically, the ambiguity surrounding consent in terms of both its wording and its use as a lawful basis for data processing obstructs data sharing in health care and research. The individual runs a risk when his data are not shared if he has not given his consent, while the data sharing is required for information about his health. He may also run a risk when he shares his data beyond the traditional care provider–care receiver relationship. When this occurs, he lacks the protection granted to him by the health provider who is bound by medical professional secrecy. When health data are not shared for research purposes, not only the individual's health but also public health may be jeopardized.

Ambiguity surrounding legal terminology not only exists in the interpretation by the member states, but also within Union legislation itself. For instance, terminology used in the GDPR varies from that used in the EHDS or AI Act. The EDPB and EDPS issue guidelines, opinions and recommendations, but these have not prevented ambiguities in interpreting concepts or delays, or even the absence of cross-border research. The GDPR has not established a uniform framework in the European Union. Member states may still maintain national exceptions to the general rules in the GDPR. Since the EDPB has indicated that this lack of homogeneity cannot be resolved in EDPB guidelines or by means of codes of conduct, the health institutions are challenged to take up the gauntlet themselves.

These observations lead to yet another issue. Though the GDPR provides for a general, risk-based and technology-neutral framework, the data protection authorities pursue this objective differently. The number of fines imposed by the data protection authorities varies throughout the European Union and data protection authorities merely follow a regulatory, rule-based approach based on compliance rather than a risk-based approach. Furthermore, several supervisory mechanisms, both general and sector-specific authorities, monitor compliance in the health sector. Moreover, the EHDS and AI Act create additional supervisory mechanisms, both at a European level and within the member states. Questions arise regarding the division of tasks among these authorities.

Conclusions

A balanced approach for the exchange of health data can be found in the following four ways. Firstly, a broad(-er) interpretation of the lawful basis of consent can facilitate secondary health research in the Netherlands and the European Union. To

this end, the granularity of consent included in recital 33 needs further clarification as regards the scope for secondary research purposes.

Secondly, the use of other lawful bases, such as the public interest and legitimate interests can be a solution for the legitimation of secondary health research in the Netherlands and the European Union. Furthermore, a separate legal ground for secondary research purposes can be a solution to resolve the issue of a proper lawful basis for health research. A separate legal ground for this research has neither been included in the GDPR nor in Dutch law yet. The EHDS contains provisions about the primary and secondary use of data. However, the concept of secondary use is not completely similar to the concept of further processing in the GDPR. With the developments in the EHDS, amendments in the Dutch legislation, in particular article 24 UAVG, as well as articles 7:457 and 7:458 WGBO, and the draft Wzl, would be needed as well.

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. In health care and research, the individual exercises the control over his data with the expression of his consent. However, he may not be able to oversee the consequences of the expression of his will. In health care, the balance can be found in the triangle of care where the formal or informal representative and the care provider assist the individual in his decision-making. In health research, the balance can be found in the objective of the GDPR that individual rights are protected whilst the free flow of data is not hampered. The focus is shifted from the individual's control over his data towards the data controller with the use of other lawful bases than consent and with a fair balance between data protection rights on one hand, and the free flow of data, on the other.

Fourthly, a risk-based approach to monitoring compliance, performed by the Data Protection Authority and sectoral supervisory mechanisms, contributes to balancing the rights and interests of individuals with data sharing for health care and research purposes. Furthermore, this approach will encourage health institutions to focus on compliance on the one hand and to balance the individual's data protection with health research on the other. At the same time, clarity is needed as to the roles and responsibilities of the various supervisory mechanisms in data protection and health. With the advent of new supervisory bodies under the EHDS and the AI Act, legal certainty is required about the boundaries of their different and perhaps overlapping roles and responsibilities.

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.

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

Firstly, I recommend that the data controller acknowledges its burden of control as regards data processing. The individual is neither able to control the processing of the data himself, nor is he able to implement the technical and organizational measures. Regardless of which lawful basis is used for data processing in health care and research, the controller must take the necessary technical and organizational measures. Furthermore, the data controller must inform the individual in a clear, transparent manner about the data processing. In sum, the focus must be on the data controller's transparency and accountability, which, in turn, will also garner the individual's trust in the health or research institution.

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 when 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. For instance, the lawful bases of the public interest and legitimate interests are used in the European Union. Additionally, 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. Furthermore, the developments in the EHDS must 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 the individual, health provider, and representative deserves further attention. In 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 up to several decades.

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 all the 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 fully controls the data himself. The GDPR does not grant the individual full control over his data either.

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 and EHDS 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.

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 are involved in showing compliance with records of data processing activities (article 30 GDPR), Data Protection Impact Assessments (article 35 GDPR), records of data breaches (article 33 (5) GDPR), and the presence of a data protection officer (articles 37 – 39 GDPR). Although the activities have proved useful, these documents alone 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 Union and the Netherlands cooperate more closely with sectoral 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 broadened 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.

Final considerations for future research

This research did not touch upon many related topics that merit future research. Firstly, future research is recommended on the principles of solidarity and reciprocity in health research. Secondly, future research is recommended on the elements of informed (ethical) consent (in the Clinical Trial Regulation) and the elements of consent in the GDPR, especially in relation to new legislative developments in the Netherlands (which incorporate the requirements of the GDPR consent).

Thirdly, future research is recommended on the interaction between the European legislation (EHDS, AI Act, Data Act, and Data Governance Act) and Dutch legislative developments (inter alia, the draft Dutch Authority over Human tissue Act, *Wet zeggenschap lichaamsmateriaal, Wzl*). Additionally, future research is recommended on

the interaction between the GDPR, the UAVG and, more specifically, sectoral health legislation.

Fourthly, future research is recommended on the compliance mechanisms by the European and national data protection authorities, as well as sectoral supervisory mechanisms. This research could include the interaction between the different supervisory mechanisms, both at a European and national level, and both by general and sectoral authorities.

Fifthly, future research is recommended regarding the individual's own role in monitoring his health. Self-tracking devices in monitoring one's health could benefit individual decision-making. However, the very same innovative technologies could compromise the individual's autonomy and informational self-determination. Further research could further unravel the individual autonomy, self-determination and informational privacy amidst the use of new technologies.

Lastly, further research is recommended on 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. A tailor-made communication strategy for different target groups contributes to the individual's feeling of trust and willingness to share health data.