AIM POSITION ON THE EUROPEAN HEALTH DATA SPACE

I. Introduction

We would like to take the opportunity to be able to provide input to the European institutions on the Regulation of the European Parliament and of the Council on European Health Data Space (hereinafter "European Health Data Space"). We have studied the legislative framework and with this paper, we draw attention to our conclusions on the proposal on the European Health Data Space.

II. Impact on Health Insurance Funds and Health Mutuals

According to the European Commission, the proposal provides rights to the insured/patient by supporting individuals to take control of their own health data, by supporting the use of health data for better healthcare delivery, better research, innovation and policy making and by enabling the EU to make full use of the potential offered by a safe and secure exchange, use and reuse of health data.[1] Health Insurance Funds and not-for-profit health mutuals are “data holders” and “users” and are thus parties in the rules on both primary use and secondary use of health data. Various provisions such as on interoperability of systems and data or on data quality have wide-ranging implications for AIM members. Health insurance funds and not-for-profit health mutuals have therefore every interest in reviewing the content of the European Health Data Space, contributing to the legislative procedure and identifying potential bottlenecks.

III. General remarks

Health insurance funds and not-for-profit health mutuals support a better use of data and therefore welcome the proposal on the European Health Data Space. AIM agrees with the huge potential that a flexible use of health data has for patient centeredness as well as improving healthcare quality and outcome. A closer cooperation in the use of health data shall aim to improve patient’s access to healthcare and allow to predict the costs of the treatments more easily (the amount to pay and the part reimbursed by the health system). The use of real-world data can drive research, cost-effectiveness

[1] https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en

analysis, treatment, and care, identify inefficient spending and empower patients through access to their own data and records. Through data collection, their organization as well as the regulation of their access and use, it is possible to develop and implement national and European strategies for AI in healthcare. The outbreak of COVID-19 has made clear that access to health data, notably real-world data, for scientific research and a coordinated interpretation is of utmost importance. Moreover, a European health data hub would increase the competitiveness of Europe in a world, where other regions are developing at high pace in this area, sometimes under less stringent data protection regimes than that of Europe. All this said the following considerations need to be taken into account:

1. Respect national data structures already in place

The EU introduces a new framework for the European exchange of health data. While creating the new EHDS framework national investments for IT infrastructure already in place needs to be respected. The news EHDS infrastructure should be fully interoperational with health data structures that have already been created in the member states. The administrative and technical requirements put on existing infrastructure to be interoperational with the new EHDS framework should be minimized as much as possible. Electronic health record (EHR) systems that have already been approved by a national body should be able to continue to be operated when the Regulation takes effect. Where applicable, EHR developed by health insurance funds should remain the preferred service.[2]

2. Costs

The implementation will entail a cost, but it seems impossible to calculate this as many specifications are missing today. The Netherlands published a financial impact analysis[3]: the total structural costs calculated for a period of 5 years for the government for the realization of the different components of EHDS are estimated at more than €1.6 billion to €2 billion. Financial support from Europe will be necessary.

[2] See for example the bill for the Electronic Data Exchange in Healthcare Act (Wegiz) in the Netherlands. A legal impact analysis, drawn up by Radboud University, shows that the Wegiz probably needs to be adjusted: https://www2.deloitte.com/nl/nl/pages/legal/articles/wegiz-stimuleert-elektronische-gegevensuitwisseling-in-de-zorg.html

[3] https://open.overheid.nl/documenten/ronl-188e974c295399237f91d9fa6053ed8b4850a371/pdf.

3. Influence of the member states for the implementation of EHDS needs to be strengthened.

AIM welcomes the fact that the Commission proposes the creation of an expert group that assists and prepares delegated acts to "enhance the interoperability of electronic health data for healthcare, building on existing European, international or national standards and experience of other data spaces". It should be noted that achieving this standardization at European level is a very complex task, and that should be a high priority for the national organizations to put the European Health Data Space into effect. Some Member States have already invested considerable amounts of human and financial resources in digital health systems which should be considered. Duplicated structures should be avoided. Delegated acts, as proposed in the regulation, are not enough as Member States would only have an advisory role. AIM members recommend introducing implementing acts, when it comes to the interoperability and in here, the examination procedure according to article 5 of the regulation 182/2011. The examination procedure has to take the opinion of Member States as it is binding.

4. Digital health/data literacy is necessary to avoid widening the inequality gap

The EU should invest in and promote the equal development of a basic understanding of digital health/data literacy and skills (e-health, m-health literacy) in the Member States for the public at large to empower the citizen in healthcare and the citizen's knowledge on their health data. Citizens need to understand that they have the right to give and revoke an approval to use their data. In addition, they must be given the tools to manage their approvals (also for digital-illiterate citizens). Digital health/data literacy and skills should be promoted in the formation for healthcare professionals and a point of attention in (continued) education. Researchers and academics should be aware of the legal framework that applies to the digital exchange of health data. The European Commission declared 2023 the year of skills. AIM emphasizes that this is an opportunity and a good momentum to work on the challenge on digital health literacy.

5. Cybersecurity is indispensable

Cybersecurity in digital healthcare and protecting information is vital for the functioning of social security organizations. Many healthcare organizations have various types of information systems such as EHR systems, e-prescribing systems or practice management support systems. If patients engage virtually with their healthcare providers, whether through inserting information in the EHR, or otherwise, patients need to understand the privacy and security policies and also how to keep their information private and secure. The staff, working in a health insurance fund of health mutual need to

understand the privacy and security policies of the organization. Regular security awareness training is essential to cybersecurity in healthcare so that members of the staff are aware of threats and what to do in case of actual security incidents. They also need to know who to contact in the event of a question or problem. In addition, the multiplication of the number of environments from which data can be accessed increases the "area" that can be attacked by hackers and thus also increases the risk of cybersecurity and privacy problems. This risk is underexposed in the EHDS proposal and requires a great deal of awareness at national and European level.

6. Prevention should be a main goal of the European Health Data Space to achieve good health

Currently, the main goal of EHDS is healthcare; it is important that the regulation also mentions prevention as an important way to achieve and obtain good health. Health data used in new technologies has the potential to realize early detection of diseases and to identify and to support groups at high risk. For example, health data used for AI can be used to identify people at risk of certain chronic diseases, e.g., diabetes. Early intervention will lead to earlier disease management and reduce strain on healthcare resources further down the line.

7. Put in place an efficient and unified certification process for the secondary use of health data

The Data protection framework and its varying implementations across member states have created an unnecessarily fragmented landscape, which has led to uncertainty. AIM welcomes that researchers, innovators and policymakers have to apply for a permit to be able to reuse health data, that accessing, and processing of health data has to be in a "secure processing environment". AIM reinforces its opinion that the secondary use of data must be anonymous and that the reason for requesting the data before authorization, as well as the way in which they will be treated, is well scrutinized. AIM would also like to emphasize that the permit process for health data should be organized effectively. When introducing a certification procedure for the European Health Data Space, lessons should be learned for example from the current problems with the certification process of the Medical Devices Regulation. It needs to be ensured that an efficient and unified certification process is put in place. In addition, data access bodies operating differently, leading to different speeds of approval or different execution of approval processes, risking different criteria setting, should be avoided.

8. Timing

The European Commission hopes for a political agreement on the EHDS in 2023. If the regulation is officially published in 2024, it will enter into force 20 days later and will apply 12 months later, being probably implemented in 2025. Certain articles will not apply until a later date (see article 72). Given the necessary preparations – both the part from the European Commission and the Member States – AIM emphasizes that the timing is not realistic. Even if it is desirable, it will be impossible to implement this within the proposed timing. AIM therefore proposes an implementation period of 5 years (on the condition that all technical details are decided within 24 months after the entering into force.

IV. Conclusions and recommendations

1 Primary use of health data

1.1 Ensure data quality in the European Health Records

AIM members welcome the efforts to strengthen the control and rights of natural persons over their personal electronic health data but raise concerns with regards to the quality of data in the European Health Records. Art. 3 (6) gives the right to natural persons to enter their electronic health data in their own electronic health record (EHR) or in the EHRs of natural persons to which they have access, through electronic health data access services or applications related to those services. With all data added by different natural persons, medical devices and wellness apps it becomes difficult to keep overview, where the data is coming from. However, for every information in a EHR it should be clear who or what is the source of the data. Hence, data quality in European Health Records cannot be guaranteed.

However, access to accurate, complete, and timely data is critical in the healthcare. It impacts patient care as well as government initiatives to improve public health services across countries. Inaccurate and duplicated information can negatively impact data accessibility and usability. Even more, it makes it impossible for patients and staff workers to trust these data and therefore to trust medical authorities.

Health insurance funds and health mutuals propose to add to article 5 paragraph 1 the following data quality requirements relevant to healthcare:

It must be ensured that relevant data (e.g. patient ID, allergies, laboratory data, medical alerts, and current medication) added to the Electronic Health Records must be

- Accurate (data depicts reality and truth).
- Validated (Data is present in the correct pattern and format and belongs to the correct domain).

- Complete (Data is as comprehensive as needed).
- Current (Data is up-to-date or as current as possible).
- Consistent (Data is the same (in meaning and representation) across different data sources).
- Identifiable (Data represents unique identities and does not contain duplicates).
- Provenance must be clear (Data is saved with its metadata (origin and update history).
- Usable (Data is present in a format that is understandable by the ones who intend to use it).
- Secure and confidential (Data is safe from unauthorized access and patient identity is kept secret wherever needed).

Important information should be highlighted. IIt could also help to categorize and mark the data depending on the reliability of source (e.g. group 1: medical practitioner + medical device, group 2: wellness app in compliance with ISO standards, group 3: wellness app not in compliance with ISO standards, data entered by the person himself, …).

1.2 Main characteristics of electronic health data categories for primary use should be clarified and only extended by Member States or in close collaboration with them

AIM requests that the main categories of electronic health data for primary use mentioned in Article 5 (1) in connection with Annex I need to be clarified. The current formulation is not specific enough and leaves much room for interpretation. For example, it is not clear what is covered by "information on health insurance" (e.g. does it include only information about compulsory health insurance, complementary health insurance, family members, contributions etc.).

AIM proposes to delete Article 5 (2) in connection with Annex I, which allows the European Commission to adopt delegated acts to amend other categories of electronic health data. It enables the Commission to add, amend of delete categories to the list of priority categories of electronic health data. Member States can only give their opinion which does not need to be taken into account. However, Member States know best the specificities of the rules for healthcare in their countries and should therefore decide about the categories in the health records or at least have the power of co-decision.

1.3 It should not be mandatory to make health data from the past electronically available

Health insurance funds and health mutuals welcome recital 9 which says that there should be no obligation to convert health data into electronic format when it is disproportionate. AIM members recommend to insert recital 9 to article 3 (4) to make it binding. It is practically impossible to make all

data from the past available. Some data from the past is lost and even, if it is not lost, it would take a lot of time and money to make all past data electronically available.

1.4 Identification management – Member States must be included in the decision

Article 9 (1) gives natural persons the right to identify electronically using any electronic identification, when having access to personal data or using telemedicine. In this context, article 9 (2) empowers the Commission to establish, by means of implementing acts, requirements for the identification and authentication mechanisms. Those implementing acts shall be adopted in accordance with the advisory procedure (article 68 (2), article 4 of the regulation 182/2011). Health insurance funds and health mutuals recommend using the examination procedure according to article 5 of the regulation 182/2011, where Member States are involved and their opinion is binding. The establishment of digital identities is extremely complex. Member states may already have established processes at national level. They should therefore at least have a say in the form of the examination process.

1.5 Distribution of tasks and competences of the digital health authority

AIM members are of the opinion that the tasks of digital health authority are too extensive. For example, one of the tasks of the digital health authority is to offer telemedicine services and to ensure that such services are easy to use, accessible to different groups of natural persons and health professionals. Article 2 (1) defines telemedicine as "the provision of healthcare services, including remote care and online pharmacies. Digital health authorities should not offer services such as online pharmacies as it is out of their competence.

2 Obligations of EHR systems and wellness apps

Self-certification for software suppliers for EHR systems and wellness apps is not sufficient

AIM members warn that the self-certification for software suppliers for EHS systems and wellness apps are too few obligations to place EHS systems on the market. Under the EHDS, a manufacturer must prepare an EU conformity assessment and affix a CE marking to the accompanying documents and in some cases to the packaging of the EHR system. Subsequently, a random check by market surveillance authorities is carried out afterwards (after an EHR system has already been placed on the market or put into operation) of compliance with the EHDS requirements for EHR systems. In some countries, national

independent accredited institutions are deployed to issue a certification prior to EU market entry, e,g, in the Netherlands, the Health and Youth Care Inspectorate can take administrative measures against manufacturers and suppliers of ICT products in healthcare that do not comply with the established Dutch standards or standards of international origin.[4] These additional requirements are important for security reasons. On the other hand, one could argue that much administrative burden, which additional requirements cost too much time, money and scarce capacity of software-experts. It's important to focus not only on theoretical interoperability but also on practical interoperability.

3 Secondary use of health data

1.1 Health data generated by wellness applications and other digital applications should not be part of secondary use of health data

Health insurance funds and health mutuals recommend that when it comes to wellness applications, they should not be part of secondary use of health data.

Health data generated by wellness applications and other digital health applications do not have the same data quality requirements and characteristics of those generated by medical devices.[5] While some of the health and wellness apps on the market have access to highly sensitive information, others may offer advice that is not supported by scientific evidence.[6]

While it is understood that medical devices need to be included within the scope of the proposal, AIM recommends excluding wellness applications at least from the secondary use of health data. Therefore, health data deriving from wellness applications and other digital applications should be excluded from Article 33(1)(f) and (n) of the proposal.

1.2 Minimum categories of electronic health data for secondary use should be clarified

Health insurance funds and not-for-profit health mutuals recommend clarifying the minimum categories of electronic health data for secondary use listed in article 33, especially points (d) and (n). Articles 33, 41 constitute a legal obligation to data holders to share as categorised in article 33. The listed categories are very broad and contain a lot of information of sensitive health data, which can lead to legal

[4] https://www2.deloitte.com/nl/nl/pages/legal/articles/de-wegiz-en-ehds-kunnen-volgens-minister-naast-elkaar-blijven-bestaan.html.
[5] https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032022-proposal_en.
[6] https://www.cencenelec.eu/news-and-events/news/2021/eninthespotlight/2021-08-30-cen-iso-ts-82304-2-guidelines-health-and-wellness-apps/.

uncertainty. This is even more important as recital 37 states that this regulation is a legal basis in the sense of article 6 and 9 (2) of the GDPR. AIM members remind that, if possible, efforts can be made to ensure that the least complex datasets and dataset combinations are used for specific projects as foreseen by the principle of data minimization in the GDPR.[7] Appropriate technical and organizational measures should be implemented to avoid re-identification of patients.[8]

Article 33 e) and m) contain human genetic, genomic and proteomic data as well as data from biobanks, which is even more sensitive data. AIM members call for a differentiated approach.

In addition, article 33, letters f) and n) contain data from wellness applications and other digital applications. As mentioned above, data generated by digital applications, are less protected than health data generated from medical devices. AIM members emphasize that natural persons have to be aware that those data, uploaded in the European Health Record, can be shared with other recipients and be processed for secondary use. Data subjects should therefore be properly informed and the possibility to opt-out should be included. A consent is only valid, if the data subject has been appropriately informed. This counts even more against the background of article 33 (5), which seem to remove informed consent.

1.3 Intended purpose to use health data for public health and social security needs to be clarified

AIM members welcome that one of the purposes for the secondary use of health data in article 34 (1) (h) is the "development and innovation activities for products or services contributing to public health or social security...". As stated in the AIM position paper from 26 April 2021, "improved health outcomes such as new medicines or a new understanding of a disease and patient centeredness, should always be the primary purpose of using health data." However, the proposal does not describe enough when a sufficient connection with public health or social security is given. It is important to protect the privacy of data of natural persons.[9]

[7] Article 89 of the GDRR.

[8] Read AIM position paper "Improvement of healthcare through the exchange of health data – But how?", 26 April, 2021; https://www.aim-mutual.org/mediaroom/improvement-of-healthcare-through-exchange-of-health-data-but-how-2/.

[9] Joint position edpb_esps on the EHDS, https://edps.europa.eu/system/files/2022-07/22-07-12_edpb_edps_joint-opinion_europeanhealthdataspace_en_.pdf.

1.4 Prohibited secondary use of health data must be described precisely to "avoid shopping"

Health insurance funds and not-for-profit health insurers recommend describing more precisely, under which circumstances secondary use of health data shall be prohibited. For example, the definition "harm" in article 35 (e) is very broad and can be interpreted in many ways as it has a legal and a moral component. In a legal context, harm is often used in the context of tort law. There are a number of different types of torts, and each one has its own specific definition of harm. For example, in the context of personal injury law, harm refers to any physical, emotional, or financial injury that a person suffers as a result of an accident or other incident.[10] It is important to organise the permit process for the secondary use of health data effectively, to avoid situations like the process related to the Medical Devices. When introducing a certification procedure for the European Health Data Space, lessons should be learned to ensure that an efficient and unified certification process is put in place. Data access bodies operating differently, leading to different speeds of approval or different execution of approval processes as well as rejections, risking different criteria setting, should be avoided.

1.5 Health data used for research and innovation need to be fully disclosed and transparent

AIM asks for the full disclosure and transparency of health data being used for research and innovation Most health care professionals and institutions are largely fixated on their efforts to provide the best patient care they can with the given resources, but others are fixated on profits. In order to ensure that health data is really used to develop health interventions that have a real added value and to build up trust, private entities should disclose to the public the cost of research and development as a result of using data being made available. It will have important implications for the negotiation of the pricing of digital tools and new treatments later on.

[10] https://isalegal.info/legal-definition-of-harm/.

1.6 Direct exchange between requester and single data holder should be voluntary

Health insurance funds and not-for-profit health mutuals are worried that a direct bilateral exchange of data between the applicant and a single data controller as described in article 49 can be mandatory. AIM members recommend to delete this article. It can lead to high workload as well as higher costs and more staffing, especially if the data holder and requester are situated in the same country, as the data holder has to do all the work.

Brussels, 7 March 2023