**The European Health Data Space and International Data Transfers: Recommendations for Trilogues**

The Global Data Alliance (GDA), whose members include numerous companies active in the health sector, offers the following recommendations for the European inter-institutional negotiations ("Trilogues") in relation to the international data transfer provisions and data storage provisions of the Proposal for a European Health Data Space (EHDS).[1] The GDA welcomes a proactive approach to digital health governance that is protective of personal data, health, as well as scientific progress and research.[2] We outlined our general perspectives on these matters in our original comments on the EHDS, reproduced in the Annex to this submission.[3] Please do not hesitate to contact Irma Gudziunaite at Irmag@bsa.org with any questions or comments.

## Introduction

As strong supporters of the EU's General Data Protection Regulation (GDPR), we underscore the critical role of cross-border data transfers in advancing healthcare research and development (R&D), the management of healthcare services and products, and the search for new treatments and healthcare solutions to address emergent health challenges.[4] Without the ability to transfer data internationally, in a manner consistent with GDPR, the ability to conduct such R&D as well as to identify and develop new treatments and healthcare solutions may be fundamentally compromised or, at the very least, undermined. As explained by public health authorities and private research organizations,[5] the ability to transfer and access knowledge, information, and data across transnational digital networks is integral to efforts aimed at meeting global and regional health challenges.

For this reason, it is of great concern that the Council's and Parliament's respective positions on the draft EHDS appear to propose new restrictions – beyond GDPR standards – on cross-border access and transfer of personal or non-personal health data. Such restrictions may have a deterrent and chilling impact on the EU as a locus of cutting-edge healthcare research and delivery, to the broad detriment of citizens and patients across the EU and beyond.

Our comments below focus on the respective texts of the EU Commission (EC), EU Parliament (EP) and Council.[6]

## Concerns and Recommendations

- **Articles 60 & 60A, Recital 64 & 64A: Local Storage Mandates for Health Data Access Bodies**. The respective texts of the EP and the Council introduce an obligation to store personal electronic health data in the territory of the EU, which the GDA opposes.
    - **EC Text**: The initial EC proposal does not include any local storage mandate, in line with the GDA recommendations.
    - **EP Text**: The EP text includes a strong local storage mandate with requirements for personal electronic health data to be "exclusively" stored in the EU territory. Not only for Health Data Access Bodies, but also for any purpose of primary use of electronic health data, the EP text mandates that the storage of personal electronic health data shall exclusively take place within the territory of the Union (Article 60a). Additionally, the EP text makes this a requirement for public procurement and Union funding of Electronic Health Records (EHR) and EHR systems (Article 60(2a))). Moreover, the EP text goes even further in mandating that public procurement candidates "duly demonstrate" they are immune to third-country law conflicting with the EU law. These new mandates contradict existing EU law. GDA respectfully urges that existing EU legal standards be maintained.
    - **Council Text**: Article 60a(2) includes a similar local storage mandate for personal electronic health data, including in cases in which such data is pseudonymised or anonymised, against GDA's recommendations, but with an exception relating to a "third country covered by an adequacy decision" under Article 45 of the General Data Protection Regulation (GDPR).

**Rationale**: The EP and Council texts go too far by introducing new local storage mandates not present in the initial EC proposal. Furthermore, the exception from such mandates in the Council text is unclear as to why transfer mechanisms under the GDPR, other than adequacy decisions, would not apply. Indeed, it has been recognised by both the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) that the provisions outlined in the GDPR are sufficient to achieve the objectives pursued by policymakers on data protection, i.e., to mitigate the risk of non-EU jurisdictions undermining EU laws, norms and values.

Taken together, EHDS Article 60A and Recital 64A in the Council text prohibit organizations from applying and relying upon GDPR various data transfer tools, such as Standard Contractual Clauses, Binding Corporate Rules or Codes of Conduct, under the EHDS.[7] This broad-based requirement is especially surprising for data that is pseudonymised or anonymised (in the Council's text), which represents another level of requirement that goes far beyond what is found in Chapter V of the GDPR. We are concerned that this departure from GDPR standards will create discrepancies between personal health data and other personal data and, even more, that is likely to sacrifice the health and data protection interests of both EU citizens and patients, and beyond.

**Recommendation:** We recommend to follow the EC's initial proposal which did not include any of these local storage mandates or, at the very least, if such mandates were contemplated, to align Article 60-60A and Recitals 64-64a with the GDPR – allowing reliance on various GDPR personal data transfers tools for the purposes of cross-border data transfers.

- **Article 61: Data Transfer Restrictions based on Limited Number or Geographical Dispersion of Data Subjects.** The three institutions are aligned on Article 61 in proposing to impose additional restrictions beyond GDPR on transfers of data to third countries where there is an (as yet) undefined possibility of reidentification through means that are "not reasonably likely to be used". As stated in Recital 64 (similar for all three institutions),[8] it may not be possible to mitigate these privacy considerations in instances involving efforts to development treatments for life-threatening or debilitating rare diseases. Accordingly, the three institutions are aligned with envisioning the development of additional protective measures pursuant to Article 5(13) of Regulation 2022/868

  **Rationale**: The GDA respectfully observes that it is precisely in instances involving such rare diseases – where it is necessary to aggregate data from patient populations in different countries and regions to assess the safety and efficacy of prospective treatments – that the ability to transfer data is critical to the protection of human health. Consistent with Article 35 of the EU Charter of Fundamental Human Rights, we urge the EU to duly account for, as well as respect and preserve the needs of patients, which – as noted in Recital 64 mentioned above – may face "life-threatening" or "debilitating" conditions in the absence of safe and effective treatments.

  **Recommendation:** We recommend to expressly permit the continuation of such transfers in the circumstances outlined in Art. 61 (and Commission's Recital 64), pending the assessment and finalization of new protective measures under Art. 5(13) of the Data Governance Act and the relevant provisions of the GDPR. We also recommend to fully account for the health and medical interests of EU patients and citizens in developing such protective measures.

- **Article 62: Data Transfer Restrictions for Anonymous Electronic Health Records.** The three institutions are overall aligned on Article 62(1) which foresees the prevention of transfers to a third country or international organisation of ("non-personal" for the EC and EP; "anonymous" for Council's) electronic health data "where such transfer would create conflict with Union law or the national law of the relevant Member State." The GDA understands that Article 62(1) would prevent cross-border transfer and access relating to ("non-personal" or "anonymous") data in specific cases where another EU law or EU member state law expressly prohibits such transfer or

access. To the extent that Article 62(1) operates in this manner, it should avoid transfer restrictions that are greater than necessary and that could unduly impede the EU's international connectivity and commerce with third countries.

**Rationale**: Unfortunately, ambiguity regarding the circumstances in which a "conflict" may arise with EU law or Member State law could invite problematic legislative interpretations stemming from the possible divergence of interpretation from EU Member-States' own Data Protection authorities (DPAs). To mitigate interpretative challenges for EU judicial and administrative authorities, we would recommend that the EU provides a detailed list of EU and Member State provisions that expressly prohibit such transfers. Absent such a legislative clarification, the EHDS proposal would face the risk of alternative interpretations that health data must be localized and/or that data transfer or access must be blocked on the basis of a wide and undefined scope of potential "conflicts" with EU law or member state law. Indeed, if data transfer or access were halted in this unpredictable and broad manner, it could raise questions regarding the EU's compliance with its international obligations[9] and impede the future ability of EU and foreign entities to engage in cross-border healthcare R&D and other activities.[10]

**Recommendation:** We recommend that the EU provides a list of the EU laws or relevant Member State laws that it currently believes would prohibit transfers (i.e., "create conflict") in the manner envisioned in Article 62.

- **Article 63: Additional Conditions for Personal Data Transfers Based on Member State Law.** Article 63 grants Member States broad authority to impose additional conditions, including limitations, on transfers of personal electronic health data to a third country or an international organisation.
  - **EC Text**: The EC initial proposal allows Member States to maintain or introduce further conditions pertaining to international access and transfer of personal data
  - **EP Text**: The EP includes the same provisions but specify such access or transfer must be granted in accordance with Chapter V of the GDPR. However, it only allows access and transfer to third countries for secondary use of electronic health data where there is reciprocity (Article 63a and Recital 64c)
  - **Council's Text**: The Council includes the same provisions as the EC and also includes the requirement that such access or transfer must be granted in accordance with Chapter V of the GDPR

  **Rationale:** The relevant recitals do not explain the reasoning behind this additional clause, which exceeds the scope and the safeguards imposed on cross-border data in GDPR Chapter V and thereby seem to create a separate regime for health data and fragmenting the general regime of the GDPR for personal data as a whole. Moreover, it undermines legal certainty necessary for healthcare research and delivery in the EU, and will likely divert resources from innovation to ensuring adherence to multiple legal regimes across EU Member States.

**Recommendation:** We urge that the EU remove this provision, which exceeds the scope and the safeguards imposed on cross-border data in GDPR Chapter V and which undermines legal certainty necessary for healthcare research and delivery in the EU.

- **Recital 15aa of the Council's text: Declaration of Consistency with International Commitments.** Recital 15aa provides that the storage of personal electronic health data referred to in Article 5 for the purpose of primary use "is located within the European Union in line with Union law and international commitments."

**Rationale:** We observe that the text departs from the explanatory memorandum accompanying the original EHDS proposal by the European Commission, which stated unequivocally that the EHDS proposal must comply with the Union's international commitments in the WTO and in bilateral trade agreements. A mandatory localization of electronic health data in the EU would rather be in violation of the EU international and WTO commitments. The GDA strongly supports the EU affirmation of an intent to comply with international obligations which *de facto* mean the deletion of the data localization mandate.

**Recommendation:** We recommend to delete the reference to the data localization mandate to reflect that those international commitments will be fully respected.

## Conclusion

We urge the EU to avoid imposing restrictive cross-border data policies as part of the EHDS, as they would have far-reaching and unintended consequences.

Using data localization mandates and unnecessary data transfer and access restrictions to isolate the EU from the global healthcare research and innovation ecosystem would not only undermine the availability of new treatments within the EU, but also EU-based medical technology, biopharmaceutical, and healthcare delivery R&D.

Incorporating such restrictions into the EHDS could significantly curtail the capacity and readiness of EU-based enterprises to respond to emergent health risks or to participate in critical R&D related to, e.g., non-communicable diseases, such as Alzheimer's disease and cancer as well as other longstanding medical challenges.

Similarly, such restrictions would likely directly impact healthcare availability in the EU to the extent that they would impede cross-border digital access to medical experts and professionals based in other parts of the world, and would undermine the ability to receive the benefits of data analytics and artificial intelligence (AI) technologies applied to broader transnational datasets that include EU-based data.[11]

[1] The GDA is a cross-industry coalition of companies that are committed to high standards of data responsibility and that rely on the ability to transfer data around the world to create jobs, innovate, conduct R&D, and contribute to the welfare of many countries, including via the development and delivery of healthcare products and services. Based in countries including Denmark, France, Germany, Hungary, Ireland, and Switzerland, as well as Australia, Brazil, Canada, Indonesia, Japan, Korea, Singapore, South Africa, the United Kingdom, and the United States, GDA members are active across more than 15 sectors and 150 countries. Together, GDA member companies employ millions of citizens across the EU in the biopharmaceutical, medical technology, and other healthcare-related industries. For more information, please see: https://globaldataalliance.org/sectors/

[2] *See* Charter of Fundamental Rights of the European Union, 2000/C 364/01, Arts. 8, 13, and 35, at: https://www.europarl.europa.eu/charter/pdf/text_en.pdf

[3] Cross-border data is critical to the development of treatments and healthcare solutions that may help diagnose, mitigate, prevent, or substantially cure a range of health conditions. *See* Global Data Alliance, *White Paper – Data Transfers under the EU Proposal for a European Health Data Space* (2022), at: https://globaldataalliance.org/wp-content/uploads/2022/08/07282022gdaeuhealthdataspace.pdf

[4] Because the GDA is focused exclusively on issues relating to cross-border data, this submission does not comment on other issues, including those relating to intellectual property rights, secondary uses of data, interoperability, or electronic health records. However, we commend to your attention to submission of other organizations in this regard..

[5] *See generally,* Global Data Alliance, *Cross-Border Data Transfers & Biopharmaceutical R&D* (2020), at: https://globaldataalliance.org/sectors/biopharmaceutical-rd/; Global Data Alliance, *Cross-Border Data Transfers & Medical Technology* (2022), at: https://globaldataalliance.org/sectors/medical-technology/; Global Data Alliance, *Cross-Border Data Transfers & Healthcare* (2020), at: https://globaldataalliance.org/sectors/healthcare/

[6] *See* European Commission, *Proposal for a Regulation on the European Health Data Space,* Interinstitutional File 2022/0140(COD) (May 3, 2022), [EUR-Lex - 52022PC0197 - EN - EUR-Lex (europa.eu)]; Council of the European Union, *General Approach on the Proposal for a Regulation on the European Health Data Space,* Interinstitutional File 2022/0140(COD) (Dec. 7, 2023), [pdf (europa.eu)]; European Parliament, *Position on the Proposal for a Regulation on the European Health Data Space,* Interinstitutional File 2022/0140(COD) (Dec. 13, 2023), Texts adopted - European Health Data Space - Wednesday, 13 December 2023 (europa.eu)

[7] The prohibition of reliance of GDPR Article 46 safeguards is reinforced in the new Recital 64A, which states that the EHDS requires "electronic health data to be stored and processed within the Union […], unless an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 applies."

[8] *See* Recital 64, which states in relevant part as follows: "Even in situations of the use of state of the art anonymization techniques, there remains a residual risk that the capacity to re-identify could be or become available, beyond the means reasonably likely to be used. Such residual risk is present in relation to rare diseases (a life-threatening or chronically debilitating condition affecting not more than five in 10 thousand persons in the Union), where the limited numbers of case reduce the possibility to fully aggregate the published data in order to preserve the privacy of natural persons while also maintaining an appropriate level of granularity in order to remain meaningful. It can affect different types of health data depending on the level of granularity and description of the characteristics of data subjects, the number of people affected or and for instance in cases of data included in electronic health records, disease registries, biobanks, person generated data etc. where the identification characteristics are broader and where, in combination with other information (e.g. in very small geographical areas) or through the technological evolution of methods which had not been available at the moment of anonymisation, can lead to the re-identification of the data subjects using means that are beyond those reasonably likely to be used. … Therefore, for these types of health data, there remains a risk for re-identification after the anonymisation or aggregation, which could not be reasonably mitigated initially. … [As regards] transfer to third countries, [t]he protective measures, proportional to the risk of re-identification, would need to take into account the specificities of different data categories or of different anonymization or aggregation techniques and will be detailed in the context of the Delegated Act under the empowerment set out in Article 5(13) of Regulation […] [Data Governance Act COM/2020/767 final].

[9] If Article 62 were applied in a manner that prohibited data transfer or access on the basis of a broad and undefined scope of potential conflicts with EU law, it could raise questions regarding compliance with the EU's transparency-related international obligations.

[10] If a court or administrative authority interpreted Article 62 to require that data transfers be prohibited on the basis of potential – but unspecified – "conflicts" with any other EU law and EU member state law, significant challenges could arise in the application of the Data Act. Without greater clarity regarding the operation of this provision – i.e., what constitutes a "conflict" – judicial or administrative enforcement of this provision could lack predictability, which could impede the ability of EU and foreign enterprises to plan their commercial, R&D, or other activities. For example, would differing legal requirements (e.g., regulatory requirements for product safety or testing; different technical standards in manufacturing processes, etc.) potentially give rise to such a conflict. While it appears that the legislation does not intend to require the prevention of data transfers in these circumstances, the drafting of Article 62 could be clarified in this regard.

[11] Requiring localization and unduly restricting transfers data in the healthcare context or unduly restricting transfers thereof would not only restrict the access to AI technologies outside the EU, but could also prevent EU-based enterprises from commercializing in other markets any AI solutions that they create via data subject to the EHDS requirements.

# Annex

# White Paper: Data Transfers Under the EU Proposal on the European Health Data Space

This Global Data Alliance (GDA) White Paper addresses the data transfer provisions (articles 61-63) of the European Union (EU) *Proposal on the European Health Data Space* ("EHDS"). The GDA is a cross-industry coalition of companies that are committed to high standards of data privacy and security and that rely on the ability to transfer data responsibly around the world. GDA members represent every sector of the global and European economies.[1]

The cross-border exchange of non-personal health data is critical to developing new biopharmaceutical treatments and improving medical outcomes for patients within the EU and beyond. We urge the Commission to avoid imposing in the EHDS restrictive cross-border data policies that would have far-reaching and unintended consequences. Using data localization mandates and unnecessary data transfer restrictions to isolate the EU from the global transnational biopharmaceutical and medical innovation ecosystem would not only undermine the availability of new treatments within the EU, but also EU-based biopharmaceutical research and development (R&D). Incorporating such restrictions into the EHDS could significantly curtail the capacity and readiness of EU-based biopharmaceutical enterprises to respond to emergent health risks or to participate in critical R&D related to Alzheimer's disease, cancer and other longstanding medical challenges. Similarly, such restrictions would likely directly impact the healthcare availability in the EU to the extent that they would impede cross-border digital access to medical experts and professionals based in other parts of the world, and would undermine the ability to receive the benefits of data analytics and artificial intelligence (AI) technologies applied to broader transnational datasets that include EU-based data.[2]

This White Paper is also accompanied by an Annex detailing the Role of Data Transfers in Healthcare Research and Delivery.

## I. Cross-Border Data Provisions in the EHDS Proposal

Below we discuss the provisions of EHDS Articles 61 to 63 in light of the cross-border data aspects of biopharmaceutical R&D, medical technologies, and healthcare delivery, among other topics.

### A. Article 61

Article 61 of the draft Proposal, entitled "Third country transfer of non-personal electronic data," provides as follows:

> 1. Non-personal electronic data made available by health data access bodies, that are based on a natural person's electronic data falling within one of the categories of Article 33 [(a), (e), (f), (i), (j), (k), (m)] shall be deemed highly sensitive within the meaning of Article 5(13) of Regulation […] [Data Governance Act COM/2020/767 final], provided that their transfer to third countries presents a risk of re-identification through means going beyond those likely reasonably to be used, in view of the limited number of natural persons involved in that data, the fact that they are geographically scattered or the technological developments expected in the near future.
>
> 2. The protective measures for the categories of data mentioned in paragraph 1 shall depend on the nature of the data and anonymization techniques and shall be detailed in the Delegated Act under the empowerment set out in Article 5(13) of Regulation […] [Data Governance Act COM/2020/767 final].

Article 61 could impact that ability of European entities to engage in transnational R&D for the benefit if European citizens and patients. This is in large part because it deems various types of non-personal data as highly sensitive personal data under Article 5(13) of the *Data Governance Act* because of a risk of reidentification upon transfer to a third country. Indeed, given that the data is non-personal, the stated rationale ("re-identification" as personal data) is puzzling. Furthermore, Article 61 seems to state that such "non-personal data" will be deemed to be "highly sensitive personal data," even if re-identification is improbable and could only be achieved using extraordinary means (i.e., "through means going beyond those likely reasonably to be used.").

Setting such a high bar for non-personal data in the healthcare context could create unintended risks and costs for the health of European citizens and patients. This non-personal data is critical to biomedical R&D efforts. For example, without the ability to exchange such non-personal data, representation and broad populace profiles from Europe could be excluded from the scope of ongoing multi-regional efforts to find treatments for emerging healthcare challenges.

It would be helpful to provide additional information on the objective criteria defining the types of supplemental protection measures, for example tokenization, anonymization, and/or blockchain, which could be used to ensure transfers to third-party countries. Clarity on these protective measures and assurances that these measures will be objectively applied and uniformly recognized across EU Member States as adequate measures to justify cross-border transfers would be welcome to ensure continuity of global biomedical research. Additional evidence or substantiation of the specific risk of reidentification cited in Article 61 would also be helpful. Finally, it is recommended that the Commission undertake a fuller examination of the potential impact of Article on the ability of EU health research organizations and healthcare providers to meet the needs of European citizens and patients – especially those suffering from rare diseases. Additional clarity on these points would be helpful and could help inform policy choices with fewer potential collateral impacts.

### B. Article 62.1

Article 62.1 of the draft Proposal, entitled "International access and transfer of non-personal electronic health data," provides as follows:

> 1. The digital health authorities, health data access bodies, the authorised participants in the cross-border infrastructures provided for in Articles 12 and 52 and data users shall take all reasonable technical, legal and organisational measures, including contractual arrangements, in order to prevent international transfer or governmental access to non-personal electronic health data held in the Union where such transfer or access would create a conflict with Union law or the national law of the relevant Member State, without prejudice to paragraph 2 or 3 of this Article.

Restated, Article 62.1 appears to allow cross-border transfers of non-personal data from a data processor in the EU to another jurisdiction, and allows access to such data, provided that the processor takes the specified measures to prevent "international transfer or government access" where "such transfer or access would create a conflict with EU or member state law". Importantly, the explanatory memorandum also underscores that the proposal should comply with the Union's international commitments in the WTO and in bilateral trade agreements.

The GDA understands that Article 62.1 would prevent cross-border transfer and access relating to non-personal data in specific cases where another EU law or EU member state law expressly prohibits such transfer or access. To the extent that Article 62.1 operates in this manner, it should avoid transfer restrictions that are greater than necessary and that could unduly impede the EU's international connectivity and ability to engage in transnational health-related R&D and services for the benefit of European citizens and patients.

Broadly speaking, the GDA is concerned that this provision would create unprecedented new restrictions on non-personal data, going beyond accepted standards of anonymization. The problem the Commission is trying to address – the specific vulnerability to re-identification of certain datasets – can be better met through a proper risk-based approach to anonymization applied by data exporters, rather than regulatory intervention.

Furthermore, ambiguity regarding the circumstances in which a "conflict" may arise with EU law or Member State law could invite problematic legislative interpretations. We urge the Commission to consider how best to mitigate interpretative challenges for EU judicial and administrative authorities through a more clear and precise provision.[3] Absent such a legislative clarification, the EHDS proposal would face the risk of alternative interpretations that non-personal data must be localized and/or that data transfer or access must be blocked on the basis of a wide and undefined scope of potential "conflicts" with EU law or member state law. Indeed, if data transfer or access were halted in this unpredictable and broad manner, it could raise questions regarding the EU's compliance with its international obligations[4] and impede the future ability of EU and foreign entities to engage in cross-border healthcare R&D and other activities.[5]

The GDA strongly supports the EU's affirmation of compliance with its existing international obligations. Consistent with those obligations, any restrictions on such transfers should be limited to what is strictly necessary to serve a legitimate public interest, be limited to the least trade-restrictive option available, and not undermine obligations to permit the cross-border provision of relevant services. We recommend that the Commission engage in deliberate consideration of the potential consequences of these cross-border data provisions; the specific legislative purposes to be fulfilled; and the most proportionate means of doing so without risking significant unintended consequences to healthcare in the European Union.

### C. Article 62.2 – 62.5

The requirements of paragraphs 2 to 5 appear tailored in a manner that create safeguards but allows, for instance, law enforcement access with sufficient due process considerations. It may be helpful to clarify the drafting of Article 62 §2 to 5 to ensure that the provisions operate in this manner. Such drafting clarifications will help ensure predictability and legal clarity, including on how the rules are going to be enforced, as well as to what will be the criteria to determine whether the measures taken comply with the law.

As drafted, some of these provisions could be read to imply that third-country government requests for data (or indeed requests from other third-country authorities) pose risks to EU organizations' IP rights in their non-personal data. The GDA is unaware of any evidence to support this interpretation. Moreover, it is unlikely that government access requests for non-personal data will infringe upon fundamental rights set out in the Charter. Lastly, as regards government data access requests, entities that handle non-personal data for healthcare R&D or healthcare delivery purposes receive very limited – if any – data access requests given the nature of the data and services at issue. Absent such risks, the rationale for the Commission's data transfer restrictions for non-personal data are difficult to discern. Therefore, we would urge that any policy options related to government access to non-personal data issues in the international sphere should ensure a level-playing field, be proportionate to the risks, and be non-discriminatory.

Moreover, given that the stated rationale for introducing these requirements is to protect non-personal data of sensitive commercial, national security or defense value, the broad application of these provisions to all non-personal data seems overbroad and heavy-handed, particularly in light of the significant disruption to EU and foreign manufacturers and producers across all sectors of the economy.

The impact of these provisions in the medical and healthcare sectors could be significant. While a request for such non-personal data is rare, the concern is that regulated entities will focus on hypothetical scenarios (however unlikely in practice) that could theoretically be implicated by the Article 62 provisions, rather than whether non-personal data in a medical or healthcare context is – in actuality – likely to be the subject of such law enforcement requests. This could mean that deidentification, aggregation, or anonymization data are no longer seen as sufficient to protect data regardless of the actual sensitivity of data in question.

Additionally, as regards Article 62(4), it would be helpful to have more clarification on the concept of minimum amount of data to be shared and of the meaning of a "reasonable interpretation" of the request.

An additional point relating to the requirement to be transparent about any requests that are received (Article 62(5)) requires the provider to inform the data holder prior to disclosure. We are certain that the Commission would wish to avoid imposing rules with regard to foreign authorities that authorities in the EU could not themselves comply with. Indeed, if a third country were to adopt similar measures than those contemplated in the draft proposal, it is worth asking whether cloud service providers would be free to notify users in that country of any data access demands they had received from EU Member State authorities.

Moreover, the Commission's definition of the 'data holder' creates confusion, notably with regards the B2B and B2G data access and sharing, as it seems based on the false premise that technical design of a related service induces control on the product generated data.[6]

### D. Article 63

Article 63 of the draft Proposal, entitled "International access and transfer of personal electronic health data," provides as follows:

> In the context of international access and transfer of personal electronic health data, Member States may maintain or introduce further conditions, including limitations, in accordance with and under the conditions of article 9(4) of the Regulation (EU) 2016/679

Article 63 seems to invite further lack of harmonization in implementing GDPR – particularly in relation to cross-border data transfers. Whereas GDPR Article 9(4) speaks of "conditions… with regard to the processing of genetic data, biometric data or data concerning health," Article 63 seeks to focus that provision exclusively in the area of cross-border data access and transfers, inviting unilateral limits to international transfers on an *ad hoc* basis. While the GDA understands the legal nexus between GDPR Article 9(4) and EHDS Article 63, it would be beneficial for the Commission to explain: (1) why it is necessary to develop this additional gloss on GDPR Article 9(4) – i.e., the underlying policy goals; (2) both the benefits and the costs/risks associated such additional cross-border data restrictions; (3) the economic and health-related impacts of such restrictions on European citizens and patients; (4) whether those policy goals can be achieved in a manner that imposes fewer restrictions on cross-border data transfers; and (5) whether there may be a better mechanism to develop a coherent approach to achieving those policy goals than simply referring to uncoordinated and *ad hoc* Member State by Member State restrictions.

## II. Conclusion

For the reasons stated above, we urge the Commission to avoid apply data localization mandates or data transfer restrictions that could significantly impact the availability in the European Union of advances in biopharmaceutical R&D and medical technologies that are critical to improved patient outcomes for Europeans. Given the consequential nature of the questions raised, we recommend that the Commission undertake a careful and deliberate consideration of the potential consequences of these cross-border data provisions; the specific legislative purposes to be fulfilled; and the most proportionate means of doing so without risking significant unintended consequences to EU biopharmaceutical R&D, medical technology development, and healthcare outcomes for EU citizens.

# Annex

## A. The Role of Data Transfers in Healthcare Research and Delivery

Numerous economic studies and surveys confirm the importance of data transfers to the EU specifically,[7] including in the contexts of biopharmaceutical R&D, medical technologies, and healthcare delivery.[8]

From a technical perspective, the seamless and responsible transfer of data across transnational IT networks enables the deployment of modern and emerging technologies and services that underpin healthcare delivery and the development of new treatments. These technologies and services, accessed across transnational IT networks, support many important health-related objectives, as summarized below with respect to: (1) biopharmaceutical and medical technology R&D; and (2) healthcare delivery, which often involves state-of-the-art medical devices and technologies. We address each in turn below.

### 1. Cross-border data transfers and biopharmaceutical and medical technology R&D

Cross-border data transfers are critical to the research, development, and delivery of new biopharmaceutical medicines and medical technology produces to prevent and treat medical conditions and improve patients' health, as summarized below:

- **Cross-border data analytics and R&D Collaboration.** Cross-border data analytics can help speed the early identification of potentially useful drug candidates, shortening discovery timelines from years to months. The health data-sets and genomic data used in this analysis can come from multiple sources, such as clinical trials, data registries, and real-world evidence, but the required expertise, technology, and computer facilities often are not in the same country as where the data originates and, indeed, may be spread among many countries. Pharmaceutical and medical technology R&D also depends on cross-border access to medical journals fand scientific collaboration, reflected in a high degree of international co-authorship and new methods of sharing research and computing resources for cross-border R&D.

- **Cross-border digitization of clinical processes.** Cross-border data flows are essential to the conduct of clinical trials. Data flows are necessary to identify and establish clinical trial sites, identify clinical trial participants, and monitor the conduct of clinical trials. Cross-border data transfers also help companies address different countries' drug regulatory approval requirements, and requirements of Independent Ethics Committees (IEC) and Institutional Review Boards (IRB). Cross-border digitization of clinical trial processes is also reflected in the growing prevalence of cloud-based clinical tools, including wearables, Internet of Things (IoT) medical devices, data exchange initiatives, and Regulatory Information Management Systems (RIMS) that support safety and efficacy reviews and regulatory compliance across multiple countries.

- **Cross-border demographic representation.** Cross-border studies are also critical to ensuring that new products are safe and effective across different demographics, populations, and regions. Cross-border cloud-enabled technologies can help improve patient access, diversity, and representation in clinical trials, given the importance of a sufficiently large and diverse population of participants. In addition, clinical trials for rare disease drug development are conducted in multiple countries to gather data from a sufficient number of qualified participants.

- **Cross-border regulatory collaboration.** Each country has their own national regulatory agency to ensure that a new medicine is safe and effective. Such agencies require clinical trial sponsors to provide the underlying clinical trial data so they can make their own assessments. As a result, even after the clinical trial data moves from the trial site to the clinical trial sponsor, it must also be able to flow to governments in whatever countries where the new medicine may be approved. Cross-border data transfers also help regulators do their jobs, as reflected in cross-border collaborative frameworks to share information in regulatory reviews among health authorities in

different jurisdictions.

- **Cross-border data transfers and good pharmacovigilance practice (GVP).** Cross-border data transfers are also key to post-marketing surveillance of approved products. This often includes cross-border reporting of data on adverse reactions with global regulators; virtual inspections of global manufacturing facilities; and submission of post-authorization safety studies in different countries.

## 2. Cross-Border Data Transfers and Healthcare Delivery via Medical Devices and Technologies

Cross border data transfers are essential to the responsible, precise, and effective delivery of healthcare via medical devices and technologies, which hold significant promise for improving patient lives through the safe and efficacious treatment of health conditions, as summarized below.

- **Cross-border data transfers and healthcare diagnosis.** Cross-border data enabled diagnostic technologies have allowed for significant improvements in the quality and accuracy of medical diagnosis. Cross-border data transfers allow for the cross-referencing of larger trans-national data sets containing relevant diagnoses (with sufficient representation across regions and time periods). In this way, cross-border access to a deep reserve of diagnostic data can facilitate more precise diagnoses, thus helping to prevent misjudgments based on inadequate information and avoiding unnecessary treatments.[9]

- **Cross-border data transfers and healthcare delivery via medical technologies.** Advances in healthcare therapy via medical technologies[10] depend to a significant degree on responsible access, aggregation, and use of health data from diverse sources. In the medical technology context, data transfers can be critical to: (a) providing relevant information to clinicians for purposes of monitoring safety and efficacy of ongoing treatments, (b) health economic analysis of therapy and patient outcomes, and (c) researching and engineering therapy improvements and innovations.

- **Cross-border data transfers and responsible AI in medical technologies.** The responsible integration of medical technologies with AI and other data analytics tools can help doctors and patients better understand and predict patterns and responses in healthcare delivery contexts. Cross-border data transfers play a critical role in allowing for the aggregation of larger, more representative datasets to which these analytical tools can be applied.[11] For example, the aggregation from various regions of surgical image data in actual clinical use or from videos recorded of surgeries anywhere in the world can be used for purposes of training and developing AI systems that help refine surgical techniques and improve healthcare outcomes.

- **Cross-border data transfers and remote health services.** Cross-border data enabled remote health services (both "telemedicine"[12] and "telehealth"[13]) also hold significant promise for improving patients outcomes.[14] This can include providers and patients located in the same country, where both provider and patient require cross-border access to overseas-based remote health platforms, portals, or other technologies that can offer the highest levels of security, privacy, and functionality.[15] More specifically, cross-border data transfers are critical to remote health services, as described below:

    - **Cross-border access to state-of-the-art cyber, encryption, authentication, and blockchain technologies** provided from cloud-based servers in another jurisdiction—protecting the privacy and guarding against unauthorized monitoring, intrusion, or data exfiltration;

- **Cross-border access to health care data analytics solutions** that can analyze local data samples against databases of relevant information gathered from all over the world—enhancing the reliability and accuracy of diagnoses and treatment recommendations;[16]

- **Cross-border telehealth collaboration and research conducted among medical researchers** and professionals inside and outside the European Union via (for example): (a) expert consultations among providers or other specialists located in different countries, (b) cross-border exchange of data with laboratories or advanced research facilities in other countries with particular expertise in different types of analysis or testing; and (c) cross-border consolidation of anonymized data sets from around the world for purposes of real-time statistical tracking, analytics, and monitoring of aggregated anonymized data—e.g., to identify health trends, epidemiological patterns, or localized disease outbreaks; and

- Depending upon medical licensure and other legal requirements, **cross-border provision to patients of consultations, remote second opinions, or other information** from a provider in one country to a patient in another; and/or **cross-border humanitarian assistance** to underserved populations around the world.[17]

---

[1] *See e.g.,* Global Data Alliance, *Creating Jobs and Trust in Every Sector of the Economy* (2020); Global Data Alliance, *Cross-Border Data Transfers Across Sectors* (2022).

[2] Requiring localization of non-personal data in the healthcare context or unduly restricting transfers thereof would not only restrict the access to AI technologies outside the EU, but could also prevent EU-based enterprises from commercializing in other markets any AI solutions that they create via data subject to the EHDS requirements.

[3] Because we understand Article 62.1 to relate to other EU or EU member state measures that already expressly prohibit data transfers, we do not understand Article 62.1 to impose a *new* obligation to prevent cross-border data transfers or access. It would be useful to clarify that Article 62 is reaffirms *existing* obligations to prevent cross-border data transfers or access, and does not create a new obligation to this effect.

[4] If Article 62.1 were applied in a manner that prohibited data transfer or access on the basis of a broad and undefined scope of potential conflicts with EU law, it could raise questions regarding compliance with the EU's transparency-related international obligations. *See e.g.,* WTO Reference Paper on Domestic Services Regulation, Art. 14 (Members shall publish "documents that provide sufficient details about such a possible new law or regulation to allow interested persons and other Members to assess whether and how their interests might be significantly affected"); General Agreement on Trade and Tariffs, Article X:1; General Agreement on Trade in Services, Article III; Trade Facilitation Agreement, Article 1. More detailed transparency obligations arise in the EU's various free trade agreements. *See e.g.,* EU-UK Trade and Cooperation Agreement, Title X. Likewise, such an interpretation could raise questions regarding compliance with commitments to permit (under the General Agreement on Trade in Services) the cross-border provision of computing services, such as cloud services, that depend upon the ability to transfer (personal and non-personal) data across borders. Article 62 mandates that such transfers be prevented, directly contradicting the EU's obligation to permit the cross-border provision of computing services. The exceptions in GATS Article XIV permitting derogations for measures "necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement" do not permit a broad override of a WTO Member's international obligations. See e.g., *China - Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products*, Appellate Body Report, DS363 (2010).

[5] If a court or administrative authority interpreted Article 62.1 to require that data transfers be prohibited on the basis of potential – but unspecified – "conflicts" with any other EU law and EU member state law, significant challenges could arise in the application of the Data Act. Without greater clarity regarding the operation of this provision – i.e., what constitutes a "conflict" – judicial or administrative enforcement of this provision could lack predictability, which could impede the ability of EU and foreign enterprises to plan their commercial, R&D, or other activities. For example, would differing legal requirements (e.g., regulatory requirements for product safety or testing; different technical standards in manufacturing processes, etc.) potentially give rise to such a conflict. While it appears that the legislation does not intend to require the prevention of data transfers in these circumstances, the drafting of Article 62.1 could be clarified in this regard.

[6] Indeed, cloud service providers have customers that are generally businesses that own and control the data. In the context of cloud services, for example, business customers are provided assurances, both contractually and technically, that they own and control their data. Therefore, cloud service providers or other entities, if defined as "data holders" under the present Draft Proposal, would then be required to share data they may not have access to or are prohibited from viewing by contractual obligations with the actual controller of the data, their business customer, which owns and controls them. In case of complex datasets which could include third-party data (such as customer's providers, sub-contractors, etc.) and for which there is no direct contractual relation with the related service provider, it is even more problematic for them to be put in such a position.

[7] *See e.g.,* Global Data Alliance, *Global Industry Statement in Support of a New Trans-Atlantic Data Privacy Framework* (2022), at: https://globaldataalliance.org/wp-content/uploads/2022/04/04072022gdaglltr.pdf
[8] All European Academies (ALLEA), European Academics Science Advisory Council (EASAC), Federation of European Academies of Medicine (FEAM), *International Sharing of Personal Health Data for Research* (2021), at https://allea.org/wp-content/uploads/2021/03/International-Health-Data-Transfer_2021_web.pdf (*hereinafter* "ALLEA, EASAC, FEAM, *International Health Data Sharing*"). EFPIA, IPMPC, MedTech Europe, and AdvaMed, *Innovation Without Borders: The Importance of Transatlantic Data Flows to Healthcare Innovation and Delivery*, Discussion Paper (2020) (hereinafter *"EFPIA, IPMPC, MedTechEurope, and AdvaMed, Transatlantic Healthcare Data Flows"*); Tania Rabesandratana, *European data law is impeding studies on diabetes and Alzheimer's, researchers warn,* Science (Nov. 20, 2019), https://www.sciencemag.org/news/2019/11/european-data-law-impeding-studies-diabetes-and-alzheimer-s-researchers-warn ; *See also, EFPIA, IPMPC, MedTechEurope, and AdvaMed, Transatlantic Healthcare Data Flows*; Hallian et al., *International Transfers of Health Research Data Following Schrems II: A Problem in Need of a Solution* (2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3688392 ; Peloquin et al., *Disruptive and Avoidable: GDPR Challenges to Secondary Research Uses of Data,* Eur. J. Hum. Genetics (2020), at: https://www.nature.com/articles/s41431-020-0596-x ; Slokenberga, EU data transfer rules and African legal realities: is data exchange for biobank research realistic? 9 Int'l Data Priv. L. 30 (2019), at https://academic.oup.com/idpl/article-abstract/9/1/30/5076710?redirectedFrom=fulltext ; Robert Eiss, Confusion Over Europe's Data Protection Law is Stalling Scientific Progress, Nature (2020), at: https://www.nature.com/articles/d41586-020-02454-7 ; PHG Foundation, The GDPR and Genomic Data (2021), at https://www.phgfoundation.org/report/the-gdpr-and-genomic-data

[9] Diagnostic technologies include capital equipment including diagnostic ECG, diagnostic informatics, implantable or disposable equipments including portable testing kits.
[10] Medical technologies include capital equipment including radiotherapy equipment for oncology treatments, implantable or disposable equipments such as insertable cardiac monitor, implantable cardioverter defibrillator, and grid mapping catheters.
[11] It is important to understand conditions of patients and prospective patients across different countries.
Diverse and representative data is critical to identify clinically relevant differences among patient cohorts to detect potential biases in treatment protocols, access, and other disparities. The more data, the more accurate, safe, and unbiased AI.
[12] An example of a telemedicine service might include an online consultation with a local doctor who makes a diagnosis and treatment recommendations after (often AI-enhanced) analysis of images of suspicious skin tissue. Michael Rucker, Health Tech Is Successful in Developing Countries, VeryWell Health (March 2020), https://www.verywellhealth.com/digital-health-developing-countries-1739155.
[13] An example of a remote telehealth service might include the WHO's efforts to make available remotely to health care providers worldwide information relating to the classification of illnesses, their causes, and symptoms. *See e.g.,* World Health Organization, *WHO Releases New International Classification of Diseases (ICD 11)* (2018), https://www.who.int/news-room/detail/18-06-2018-who-releases-new-international-classification-of-diseases-(icd-11).
[14] Broadly understood to involve the provision of remote clinical services to support patients, "telemedicine" includes the use of electronic information and telecommunications technologies to support and promote long-distance clinical health care, and patient and professional health-related education. "Telehealth" has been defined to cover a *broader* scope of services, including remote non-clinical services, such as provider training, administrative meetings, and continuing medical education. *See e.g.,* World Health Organization, *Telemedicine—Opportunities and Developments*, Report on the Second Global Survey on eHealth (2010), https://www.who.int/goe/publications/goe_telemedicine_2010.pdf.
[15] In some contexts, telemedicine services offered by a provider to a patient within the same country may nevertheless involve ***cross-border*** access to a secure remote health technology hosted in another country. Such cross-border technology access may be necessary to offer a secure provider-patient interaction and to add new insights and functionality to diagnoses and treatment recommendations via AI-enhanced data analytics involving larger trans-national data sets. Relatedly, because internet traffic between providers and patients often transits among computing equipment and servers across borders, cross-border data transfers may be relevant to remote health services even in cases in which the remote health technologies are stored on servers in-country. See e.g., Casalini and Lopez González, *Trade and Cross-Border Data Flows*, OECD Trade Policy Papers (2019), http://dx.doi.org/10.1787/b2023a47-en (explaining that, "[t]he internet is a global network of computers, each with its own Internet Protocol (IP) address. When a file is sent from a computer in Country A to a recipient in Country B it is first broken down into different 'packets' …marked with the IP address of the sender, that of the recipient and a code identifying the sequence in which the packets are to be reassembled at destination. Once the packets are ready, they leave the origin computer, crossing different networks and taking different routes to destination.…In some instances, what might seem to be a domestic transfer involves a cross-border flow.")
[16] For example, algorithms can be trained to distinguish benign and malignant cancers based on a referential analysis of thousands of images of benign and malignant tissue samples, resulting in more accurate detection rates than a dermatological oncologist. See e.g., Computer Learns to Detect Skin Cancer More Accurately Than Doctors, *Agence France Presse* (May 2018), https://www.theguardian.com/society/2018/may/29/skin-cancer-computer-learns-to-detect-skin-cancer-more-accurately-than-a-doctor; Charles Towers-Clark, The Cutting-Edge of AI Cancer Detection, *Forbes* (April 2019), https://www.forbes.com/sites/charlestowersclark/2019/04/30/the-cutting-edge-of-ai-cancer-detection/#43acb1b67336; Taylor Kubota, Deep Learning Algorithm Does as Well as Dermatologists in Identifying Skin Cancer, *Stanford News* (January 2017), https://news.stanford.edu/2017/01/25/artificial-intelligence-used-identify-skin-cancer/.
[17] According to the WHO, "telemedicine networks around the world deliver humanitarian services on a routine basis, many to low-income countries. These networks provide tele-consultations for physicians and other health professionals needing advice about the clinical management of difficult cases, and some also provide education." *See* World Health Organization, Long-Running Telemedicine Networks Delivering Humanitarian Services, *Bulletin of the World Health Organization* (2012), https://www.who.int/bulletin/volumes/90/5/11-099143.pdf.