Supplemental Statement on the draft EHDS Regulation - May 2023

The Association of Clinical Research Organizations (**ACRO**) represents the world's leading clinical research and technology organizations, which among them conduct or support the conduct of a majority of industry-sponsored clinical trials in the European Union (**EU**). ACRO welcomes and is generally supportive of the proposed draft European Health Data Space (**EHDS**) Regulation.

To ensure a workable and non-ambiguous framework for the EHDS ACRO sets out some issues for further consideration and (associated) policy considerations for EU legislators.

1. **Ensuring harmonization with existing EU laws including the General Data Protection Regulation (GDPR) and the new laws within the framework of the EU Digital Strategy**. It is imperative that the provisions and definitions in the EHDS Regulation, (and also the proposed delegated acts), are aligned with existing EU and Member State laws including, for example, the GDPR and other (proposed) laws within the EU's new digital regulatory framework such as, the Data Act, and the AI Act.

2. **Scope of the EHDS**. It is important to establish clearly what is the scope of the EHDS Regulation, in terms of:

    a) who would qualify as a 'data holder' under the EHDS Regulation. In particular, it should be confirmed: (i) if a processor (as defined under the GDPR) could never qualify as a data holder under the EHDS Regulation; and/or (ii) if the EHDS Regulation could apply to a data holder located outside of the EU;

    b) what data would fall within scope to be disclosed/ requested and how a data holder may limit or have input into such a request and ensure a fair decision process (by the health data access bodies (**HDAB**)); and

    c) the purposes for the processing, which as drafted are very broad and high-level. This is particularly important to ensure that data holders understand the relationship between the GDPR legal bases for the collection of personal electronic health data and the legal bases of the EHDS Regulation for the secondary use of that data and the HDABs when assessing an application can ensure the data user will meet the requirements and process electronic health data within the envisaged scope of a particular purpose.

3. **Individuals Rights**. An opt-out mechanism has been proposed by the Committee on the Environment, Public Health and Food Safety (**ENVI**) and the Committee on Civil Liberties, Justice and Home Affairs (**LIBE**)[1] (i.e., the two Committees leading on the EHDS Regulation file), to

[1] Draft report of February 10 2023 from ENVI and LIBE.

enable individuals to opt-out of having their electronic health data processed for secondary use purposes. While ACRO acknowledges the importance of preserving such privacy rights, it considers that this right to opt-out should only be available to individuals at the time of entry into a clinical trial and with respect to the electronic health data generated during the clinical trial. The alternative i.e., the ability for individuals to exercise this right at any time would not only be incredibly burdensome for data holders, but could conflict with data use agreed in the Informed Consent, or possibly violate data retention and other requirements of the Clinical Trial Regulation. In this regard ACRO reiterates the importance of clarifying the relationship between the GDPR and the EHDS Regulation, in particular the application of Article 23 of the GDPR within the context of the EHDS Regulation.

4. **Data Localization.** ENVI and LIBE[2] (i.e., the two Committees leading on the EHDS Regulation file) have proposed provisions in the EHDS Regulation mandating that:

   a) the processing of electronic health data be "*exclusively within a secure location or locations within the [EU]*" - albeit without prejudice to Chapter V of the GDPR; and

   b) where HDABs (and other public procurers) procure or fund services from EHD-processing organizations in the EU, those organizations store the electronic health data in the EU and demonstrate that they are not subject to third country laws which conflict with EU data protection laws.

   To avoid stifling secondary research – one of the key objectives of the EHDS Regulation – the requirement to store electronic health data in the EU should be removed i.e., the focus should be on ensuring the security of the electronic health data irrespective of location. In particular, the proposed restrictions outlined in (a) and (b) above should be further developed so as to take into consideration cloud-based services which may be subject to special contractual obligations that overcome the challenges of conflicting third country laws even where the data are not physically stored in the EU[3]. It would then be the case that electronic health data could be stored in a secure environment, irrespective of the geographical location.

5. **Technical Standards and Formatting of data**. While the benefits of promoting interoperability of the new electronic health data platforms are clear, as drafted there is insufficient technical information in the EHDS Regulation as to how in practice will data be uploaded and shared. The publication of information in this regard should be prioritized as meeting these obligations could potentially be very time and resource intensive for data holders.

[2] Draft report of February 10 2023 from ENVI and LIBE.

[3] The existing French Health Data Hosting certification scheme (Hébergeurs de Données de Santé) permits cloud service providers to host personal health data outside of the EU subject to the implementation of strict requirements around data security, confidentiality and accessibility. Likewise, a joint paper published in response to the proposed data sovereignty requirements in the Cybersecurity Certification Scheme for Cloud Services was signed by a number of Member States to ensure applicability of strict EU data storage requirements where the data are not hosted in the EU.

In particular, further clarity is needed in respect of the following:

(a) How in practice compliance with the technical requirements can be met without data holders having to engage in extensive exercises to convert all electronic health data (including medical images) into the required format, particularly given the 2-month period for producing the requested data.

(b) What constitutes "anonymous" and "pseudonymous" data (i.e., given differing approaches across the EU) and the factors a data user must demonstrate in its application in order to justify its need for pseudonymized data as opposed to anonymized data. (The ENVI and LIBE Committees should be aware of decisions by the European Court of Justice in 2016 and 2023 holding that "key-coded" clinical trial data should not be considered sensitive personal data.)

6. **Protecting Confidential Information and Intellectual Property Rights (IPR)**. The protection of IPR is a key concern for data holders and whilst the EHDS Regulation requires that IPR and trade secrets are respected when responding to data access and disclosure requests, the EHDS Regulation is silent in regards to commercially confidential information (CCI). This is not consistent with other EU regulatory proposals, such as the Data Governance Act, which include carve-outs for CCI and proposals from the EU Council to refuse data sharing requests under the proposed Data Act where a data holder can demonstrate it will likely lead to serious economic harm. ACRO recommends that the EHDS Regulation be clarified to exclude CCI from the scope of the Regulation.

7. **Data permits.** A data permit will grant access to multiple datasets from one or more data holders, either directly or through a HDAB, for a specific permitted use. However the EHDS Regulation does not address in sufficient detail whether the scope of the data permit can be subsequently revisited or amended and what will happen in the event that there is disagreement on whether a particular use is covered in the data permit (e.g. an appeal mechanism or data permit review procedure). ACRO recommends that the EHDS Regulation allow for a process by which data permits can be reviewed and appealed.