ACRO Innovate Advocate Collaborate

April 17, 2024

Matthew G. Olsen
Assistant Attorney General for National Security
U.S. Department of Justice
National Security Division, Foreign Investment Review Section
175 N St. NE, 12th Floor
Washington, DC 20002

RE: ACRO comment on:
Provisions Pertaining to Preventing Access to Americans' Bulk Sensitive Personal Data and U.S. Government-Related Data by Countries of Concern
Docket No. DOJ-NSD-2024-0002

The Association of Clinical Research Organizations (ACRO) represents the world's leading clinical research and clinical technology organizations. Our member companies provide a wide range of specialized services across the entire spectrum of the development of new drugs, biologics, and medical devices—from pre-clinical, proof of concept and first-in-human studies, through post-approval, pharmacovigilance, and health data research. ACRO member companies manage or otherwise support a majority of all biopharmaceutical sponsored clinical investigations worldwide and advance clinical outsourcing to improve the quality, efficiency, and safety of biomedical research.

General Comments

First, the member companies of ACRO strongly support the purposes of President Biden's Executive Order (EO) and the subsequent Advanced Notice of Proposed Rulemaking (ANPRM) from the Department of Justice (DOJ) to protect national security and the privacy of US persons against malign foreign actors. We also appreciate the commitment of the United States to "promoting open, responsible scientific collaboration to drive innovation… [and] supporting a vibrant global economy by promoting cross-border data flows to enable international commerce and trade…"

As mentioned, the member companies of ACRO are involved in a majority of industry-sponsored clinical trials, which are aimed at the development of new drugs, devices, and treatments for the patients who need them. The conduct of such research is a global enterprise, with clinical trial data routinely gathered from participants across every continent except for Antarctica. The regulation of these clinical trials is generally approached in a harmonized way by national regulatory bodies such as the U.S. Food and Drug Administration (FDA), the European Medicines Agency (EMA), and the National Medical Products Administration (NMPA) of China, which is facilitated by the trans-national regulatory agreements arrived at by way of the International Conference on Harmonisation (ICH). ACRO members have established systematic, global compliance mechanisms and controls to protect the rights, safety, and welfare of clinical research participants as 'human subjects' and to safeguard their privacy and information security as 'data subjects.'

The review by regulators of clinical trial data meant to support the approval of new drugs and medical products routinely includes the data of trial participants from multiple countries. For example, a data package submitted to the FDA for review of the safety and efficacy of a new drug might contain trial data collected from several hundred to perhaps 30,000 or more persons in the U.S., Europe, Africa, and

South America. Similarly, data reviewed by the NMPA for the licensing of a new drug in China might include clinical trial data collected in the U.S. and Europe, as well as from clinical trials in China.

Clinical trial data is provided by participants whose informed consent makes clear that their data will be used only in a responsible and ethical manner, including review by regulatory authorities. It is important to note that clinical trial data submitted to regulatory authorities is anonymized and aggregated, does not include biospecimens, does not include personal identifiers, and does not include personal health data as defined at 45 CFR 160.103 (HIPAA).

Specific Comments

Question 2 asks, "Should the Department of Justice treat data that is anonymized, pseudonymized, or encrypted differently?" ACRO believes the answer is, yes – this is consistent with the principal regulatory regimen for the health data of U.S. persons, under which health data de-identified according to the standards of HIPAA is not regulated by the Department of Health and Human Services.

In advocating for the exemption of de-identified data, we note that the HIPAA standard allows for attachment of a re-identification "key" as long as the recipient of the data set does not have access to the code and has no means of re-identifying the data. An analogous interpretation can be found in the European Union where the European Court of Justice has, on two occasions, held that absent possession of a "key," such 'pseudononymized,' key-coded data may not be subject to the requirements of the General Data Protection Regulation (GDPR).[1]

ACRO takes seriously the DOJ's concerns about countries of concern using data analysis techniques and/or AI to "extract, re-identify, link, infer and act upon" sensitive information. However, we would note that even if a transfer of a key-coded, aggregated clinical trial data set to a recognized national drug regulatory agency for the purpose of evaluating the safety and efficacy of a yet-to-be-approved medical product were considered a *covered data transaction*, the key-coded data set would not include identifiers that could be *linked* with other available information. Further, such transfers impose detailed confidentiality obligations upon the regulatory agencies and other recipients; compliance with such obligations underpins international cooperation in the pursuit of biomedical research and the regulation of biomedical products.

Since clinical trial data accessed from or transmitted to countries of concern is transmitted or accessed only in anonymized and aggregated form, ACRO believes that clinical trial data per se should be exempted from regulations developed under the ANPRM [Question 45]. Such data may be used not only for submission to regulatory authorities, but also to improve operational efficiencies in clinical trials, (e.g., improving protocol design, reducing patient burden, etc.,) and/or used for general research as defined at 45 CFR 164.501.

---

[1] European Court of Justice – Case C-582/14 *Breyer v Bundesrepublik Deutschland*, October 19, 2016 https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62014CJ0582

General Court of the European Union – Case T-557/20, *SRB v EDPS*, April 26, 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62020TJ0557

Not only is this data anonymized and aggregated, but it is also highly unlikely to meet a definition of "bulk" data. Further, we note that ACRO member companies already deploy the security requirements that the EO stipulates would mitigate risks; that is, "(1) organizational requirements (e.g., basic organizational cybersecurity posture), (2) transaction requirements (e.g., data minimization and masking, use of privacy-preserving technologies, requirements for information-technology systems to prevent unauthorized disclosure, and logical and physical access controls), and (3) compliance requirements (e.g., audits)."

With member companies that may have personnel and back-office operations in one or more of the countries of concern, ACRO appreciates the exclusion of intra-entity transactions incident to business operations, as illustrated in Example 55.

In Conclusion

Again, ACRO strongly supports the purposes of the EO and ANPRM to protect national security and the privacy of US persons against the malign intentions and actions of countries of concern, while at the same time being careful to not inhibit crucial data flows or to establish new rules for cross-border transfers in general.

We thank the DOJ for the prompt issuance of the ANPRM and look forward to further dialogue about how best to accomplish the protection of US persons without impeding the conduct of clinical research that advances the health of patients around the world.

Please feel free to contact me at dpeddicord@washingtonhealthstrategies.com for further information.

With best regards,

Douglas Peddicord, Ph.D.
Executive Director