Brigham and Women's Hospital
Founding Member, Mass General Brigham

HARVARD
MEDICAL SCHOOL

MULTI-REGIONAL
CLINICAL TRIALS
THE MRCT CENTER of
BRIGHAM AND WOMEN'S HOSPITAL
and HARVARD

Matthew G. Olsen
Assistant Attorney General for National Security
U.S. Department of Justice,
National Security Division
950 Pennsylvania Avenue NW
Washington, D.C. 20530

November 29, 2024

Re**: DOJ-NSD-2024-0004-0001**
Proposed Rule: Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons

Submitted electronically via Regulations.gov

Dear Assistant Attorney General Olsen:

The Multi-Regional Clinical Trials Center of Brigham and Women's Hospital and Harvard ("MRCT Center") appreciates the opportunity to comment on the proposed rule entitled "Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons" (the "Rule"), published at Fed. Reg. on October 29, 2024, by the National Security Division of the Department of Justice. This proposed rule addresses efforts to safeguard and harmonize access to personal data, signaling an important step toward addressing the exploitation of data in the service of national security.

The MRCT Center is a research and policy center that seeks to improve the ethics, conduct, oversight, and regulatory environment of international, multisite clinical trials. Founded in 2009, it functions as an independent convener to engage diverse stakeholders from industry, academia, patients and patient advocacy groups, non-profit organizations, and global regulatory agencies. The MRCT Center focuses on pre-competitive issues to identify challenges and to deliver ethical, actionable, and practical solutions for the global clinical trial enterprise. The responsibility for the content of this document rests with the leadership of the MRCT Center, not with its collaborators nor with the institutions with which its authors are affiliated.[1]

As a research and policy center dedicated to international clinical research, we are in no position to judge the adequacy or implications of the proposed Rule on national security. We do wish, however, to comment briefly on its implications for public health and medicine. As we have observed in the recent COVID-19 pandemic, access to international data is critical in any assessment, evaluation, understanding, and analysis of certain diseases, including infectious diseases. Restriction of data in one direction will almost certainly limit reciprocal access to data. Below, we propose limited recommendations to protect global public health needs and the advance of science and medicine that we hope will be considered and balanced against the need for robust personal and security protections.

[1] Brigham and Women's Hospital, Mass General Brigham, Harvard Medical School, and Harvard University.

Recommendations

1. E*xplicit exceptions for international public health emergencies*

   Public health emergencies demand timely data-sharing. We recommend that the Rule explicitly include a public health exception that aligns with defined internationally accepted frameworks (e.g., a declaration by the World Health Organization of a Public Health Emergency of International Concern), allowing critical research to proceed unimpeded during crises. Transparent exemption processes should define timelines for routine exception requests while providing expedited pathways for emergencies. Any exception should include provisions to ensure ethical and security standards are maintained regarding how data will be collected, transferred, stored, analyzed, and shared to demonstrate transparency and compliance.

2. *Exception pathway for approved trusted data brokers*

   Some multilateral and international partnerships involve the ongoing exchange of data, and strict prohibitions will disrupt these collaborations. We recommend further consideration of a general exception for a trusted data broker (e.g., WHO, Uppsala Monitoring Centre) where security and privacy provisions are well-established and subject to a data use agreement (DUA) appreciating that data from the US and countries of concern will be aggregated and processed. In this case, it would be expected that results will be shared with countries (including potential countries of concern) that contribute data. In these cases, there is always a concern that the final recipient of the result may reverse engineer some data and this is difficult to future-proof. In such cases, the final actor(s) (e.g., those who reidentified or misused data) should be held accountable, not the trusted data partner. The data partner should be accountable for their own processes, actions, and compliance with executed agreements and commitments.

3. *Exception pathway for approved research collaborations*

   For some research collaborations including those involving global partners, LMICs, and other organizations and geographies, a formal approval pathway for an exception to the proposed Rule should be available when federated analyses of data are not possible. Such a pathway should require applicants to demonstrate compliance with ethical and security standards, including how data will be collected, transferred, stored, analyzed, and shared, and an expectation that only minimum necessary data will be shared. In this case, the exception pathway is envisioned to pertain to a specific research project.

   This last pathway is particularly important as there is currently no path to permit non-federally funded research that does not qualify for an exemption under either §202.510 or §202.511 (permitting certain data transactions associated with clinical investigations that support obtaining or maintaining drug, biological product, and medical device product regulatory authorizations). Public health research, epidemiologic studies, pre-clinical, and other research—funded by both federal and non-federal funders—are necessary.

4. *Alignment with international standards*

In each of the examples above, and in other sections of the proposed Rule, we recommend explicit mention of global security standards to streamline compliance and avoid conflicting obligations. The rule should require entities seeking licenses to (1) demonstrate compliance with security frameworks such as NIST, ISO, FISMA, HITRUST, CIS, and other appropriate standards and (2) commit to updating their processes to remain compliant with any future revision of those standards. In the specific case of clinical research, we suggest that the inclusion of GDPR and equivalent regulatory standards be considered as international expectations for the sharing of personal data.

We suggest further clarification of the standard used for "de-identification" as applicable to the Rule. The definition of de-identification per HIPAA differs from other interpretations and does not conform to international standards. Is retention of a "code" that would permit reidentification permissible, and if so, under what conditions? Is the transfer of a limited data set permissible, and if so, what entity provides for that permission (e.g., an institutional review board?) Similarly, the Rule should define the terms "anonymized," "pseudonymized," and "encrypted," as applicable to the Rule.

5. *Definition of "covered person" in §202.211*

At the same time, the definition of "covered person" in §202.211 should be refined to avoid both under- and overextension. The logic behind restricting the definition to entities that are "50 percent or more owned, directly or indirectly, by a country of concern, or that is organized or chartered under the laws of, or has its principal place of business in, a country of concern," presumes that the same entity, at 49% ownership, would be exempt from the Rule despite the fact that all the same security concerns would be operative. At 49% (and far lower), the "covered person" of concern may even have controlling interests in the entity.

Similarly, the Rule should consider distinguishing "covered persons [or entities]" who/that are ethical and compliant participants (exempted per our proposed recommendations above) to prevent undue restrictions on legitimate research.

6. Clarification of section 202.241

Personal health data is defined in section 202.241 as "*health information that relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual."* However, data that "relate[] to" "past, present or future physical or mental health or condition" is extremely broad and ill-defined; indeed, one might posit that the definition of data that relate to a future condition cannot be defined. The MRCT Center suggests that this definition be revised to "information that directly or indirectly identifies an individual," or some equivalent alternative.

7. *Clarification of section 202.504 – Exempt Transactions - Official Business of the United States Government*

The MRCT Center agrees with the exemption from activities described in section 202.504, but we are concerned that most basic, translational, and clinical research is not funded exclusively by

either federal or non-federal dollars. The implications of the last sentence of this section ("*The contract with the foreign laboratory and the employment of the researcher are exempt transactions but would be prohibited transactions if they were not part of the federally funded research,"* therefore, is problematic. We urge the final Rule to clarify that all research activities specifically conducted under a federal grant, contract, or agreement be rendered exempt from the Rule.

8. *Extension of expectations—and exemptions—to other entities involved in clinical and other research*

   It is important to note that medical research involves many entities in addition to research organizations and their funders. Thus, the Rule should clarify whether and if certain requirements apply to these other entities. For example, in clinical research, identifiable data may be necessary for an institutional review board (IRB, or research ethics committee, REC) to review and retain to determine the safety and efficacy of a medical product; that IRB may be independent to any entity conducting or funding the research. Clinical research organizations, technology companies, medical record companies, and others may need to, or be required to, maintain records to comply with in-country regulations. In each case, the Rule should clarify the responsibilities of these additional entities.

9. *Consideration of "'omic" research*

   The preamble to the NPRM suggests that the DOJ is considering the further application of this Rule to 'omic research (e.g., epigenomic data, glycomic data, lipidomic data, metabolomic data, meta-multiomic data, microbiomics data, phenomic data, proteomic data, and transcriptomic data.) We believe it is premature to consider this broad expansion in the absence of public comment or an understanding of the risks of these data to personal or national security.

10. *Funding the Rule and Penalties*

    Financial incentives, such as federal grants tied to investments in compliance infrastructure, could offset the costs for small and medium entities. Compliance costs and penalties should be fair and proportional to encourage compliance without discouraging collaboration. Ideally, enforcement actions should include a defined appeal process for violation

11. *Planning for implementation*

    Many specific parts of the rule will require further guidance and resources to permit organizations, including research entities to comply. Issuance of these documents will be essential prior to the effective date of the regulation.

    We recommend. that the final rule clarify that these provisions will be prospective with an effective date of the regulation of adequate time to ensure compliance.

12. *Regular review of the Rule, including an opportunity for public comment*

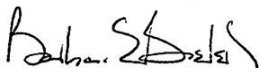
We recommend that the Rule mandate periodic review to assess its efficacy, limitations, and costs, as well as its impact on individual and public health and health equity. The evolving methods and range of research, including the use of AI in research, necessitate periodic review. These reviews should engage diverse stakeholders, including researchers, ethics boards, public and private entities, and public health organizations, and include an opportunity for public comment. Public review should be more frequent (e.g., bi-annually) during the initial phases of implementation, tapering in frequency unless there are significant changes. At that time, the list of countries of concern should be evaluated regularly to reflect geopolitical changes and prevent unintended impacts on global collaboration.

13. *Planning for implementation*

We recommend. that the final rule clarify that these provisions will be prospective with an effective date of the regulation of adequate time to ensure compliance.

The recommendations outlined can help refine and operationalize this proposed rule, supporting the DOJ's goal of enhancing U.S. privacy protections and national security. By integrating these considerations, the rule can better address security concerns while the advancement of science, medicine, and individual and public health.

Respectfully submitted,



Barbara E Bierer, MD
Faculty Director, MRCT Center

Smith Center #771, 1350 Massachusetts Ave, Cambridge, MA 02138
Tel: 617-827-7413 | Email: bbierer@bwh.harvard.edu
75 Francis Street, Boston, MA 02115
www.MRCTCenter.org