Biotechnology Innovation Organization
1201 New York Ave., NW
Suite 1300
Washington, DC, 20005
202-962-9200

April 19, 2024

By electronic submission

Docket No. NSD 104
Matthew G. Olsen
Assistant Attorney General for National Security
National Security Division
Department of Justice
Washington, D.C.

BIOTECHNOLOGY INNOVATION ORGANIZATION

Advance Notice of Proposed Rulemaking re:

Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern

The Biotechnology Innovation Organization (BIO) welcomes the opportunity to provide comments in response to the Department of Justice's March 5, 2024 Advance Notice of Proposed Rulemaking relating to the implementation of the February 28, 2024 Executive Order "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern."

The present submission is intended as a constructive first step toward a more collaborative approach with the National Security Division of the DOJ in the development of rules implementing the February 28 Executive Order, ensuring that U.S. individuals' data is appropriately secured from being used and exploited by countries of concern.

BIO believes that together and with appropriate consultation with other relevant parties, the U.S. Government can develop effective national security measures that strengthen the legitimate protections of U.S. individuals' privacy rights and health-related data, while also safeguarding the responsible use of this data to accelerate and drive biomedical research in the United States. We believe that rules can and must be structured in a manner that preserves U.S. leadership in the life sciences and in the development of cutting-edge biopharmaceutical treatments for patients and their families around the world.

BIO stresses the importance of striking the right balance between legitimate national security concerns and the promotion of a predictable, reliable and secure global legal ecosystem that allows for the responsible and secure sharing of data essential to promoting scientific collaborations, driving innovation, and enhancing overall public welfare through the development and delivery of innovative biotherapeutic treatments. BIO, therefore, encourages the National Security Division of the DOJ to carefully consider rules and calibrate actions to minimize risks and disruptions to the global, innovative biopharmaceutical research ecosystem.

Biotechnology as a National Security Imperative

BIO believes that biotechnology is a national security imperative.[1] The United States and our allies need a robust and vibrant American biotechnology industry. Biotechnology is a vital strategic asset that is essential to strengthen and protect our public health generally, and as well in our response to future pandemics and the potential for bioterrorism. It is also an essential element of our ability to project abroad the principles and benefits of a free and democratic society.

The capabilities and capacity to create, manufacture, and distribute state-of-the-art newer and better medicines and vaccines is the foundation for America to continue its essential role as the "World's Medicine Chest." Securing and advancing our pre-eminence in biomedical innovation and biomanufacturing are key components of a multi-prong approach at BIO to secure and advance this strategic imperative in biotechnology.

In addition to our commitment to securing and advancing our pre-eminence in biomedical innovation and biomanufacturing, BIO supports carefully calibrated policy measures that aim to secure American individuals' bulk sensitive personal data from countries of concern that may use and exploit this data to the detriment of U.S. national security interests. We encourage the National

[1] https://www.bio.org/press-release/biotechnology-national-security-imperative-says-bio-ceo

Security Division of the DOJ to consider input from our sector as the Division continues its efforts to clarify the process for implementing this authority.

The Convergence of Biotechnology and Digital Transformations to Drive Life Sciences Innovation

Healthcare is experiencing a major paradigm shift, from traditional one-size-fits-all medical care to personalized medicine tailored to the genomic, molecular, and lifestyle characteristics of individual patients. Unlocking the power of healthcare data to fuel innovation in medical research is at the heart of today's health care revolution, where medicine is increasingly a collaboration between data science and clinical science realms. Harnessing health data offers biopharmaceutical companies deeper understanding of disease pathways and ultimately helps develop targeted treatments with improved efficacy and safety. As a result, cellular therapies, gene therapies and genome editing with the potential to cure once incurable diseases are a reality today. The pipeline of biopharmaceutical innovation is rich with these transformative therapies that would not exist were it not for this remarkable convergence of modern biotechnology and the digital sciences.

The ability to timely and efficiently access and leverage health data to drive biomedical research – while appropriately protecting patient privacy - is critical for life science companies engaging in research and development both domestically and internationally. Policies restricting data collection, use, and sharing for healthcare and research purposes may hinder coordination and collaboration amongst research partners globally and, as a result, may impact the American biopharmaceutical industry's ability to rapidly develop and deliver breakthrough therapies to patients around the world. Accordingly, policies restricting data transfers - if not carefully calibrated - may disrupt ongoing research and development activities, frustrate global collaborations, and compromise U.S. leadership in the life sciences.

The U.S.-based biopharmaceutical industry delivers breakthrough innovations globally and we believe that harnessing health data for biomedical R&D is and can continue to be done while also protecting legitimate national security interests. Our comments and observations presented below serve to highlight how certain proposed rules in this ANPRM may impact current and future research endeavors, to the detriment of scientific innovation in the U.S. and our ability to remain world leaders in biopharmaceutical innovation. Notwithstanding, we are confident that there are definable and tailored measures that will not only support U.S. led biopharmaceutical innovation and accelerate biomedical R&D but will support the collective efforts to promote and strengthen national security and the protection of sensitive data of U.S. individuals.

Comments re: bulk volume thresholds

BIO appreciates the DOJ's efforts in the ANPRM to develop calibrated measures defining volume thresholds for each category of sensitive personal data, as opposed to an absolute prohibition on any transfer.

However, for reasons highlighted in the paragraphs that follow, biopharmaceutical firms, from small- and medium-sized biotech companies to multinational biopharmaceutical companies, are likely to exceed the minimum bulk volume thresholds that are proposed in the rules in the normal course of their research and business operations and, thus, potentially risk engaging in prohibited bulk volume transfers of sensitive personal data of U.S. individuals.

The minimum volume thresholds proposed, particularly when considering the proposal to aggregate transfer volume over a 12-month period, can easily be exceeded by U.S. biopharmaceutical companies as a result of conducting innovative global clinical research programs or as a result of seeking marketing authorizations from regulatory authorities in countries of concern.

Regarding clinical studies, U.S. biopharmaceutical firms routinely use, collect, process, disclose, and maintain data on U.S. individuals to support biopharmaceutical research efforts. Clinical research efforts in the U.S. are conducted in accordance with the Federal Policy for the Protection of Human Subjects under part 46 of title 45 Code of Federal Regulations, good clinical practice guidelines (GCPs) issued by the International Council for Harmonisation of Technical Requirements (ICH) for Pharmaceuticals for Human Use, and the human subject protection requirements of the FDA under parts 50 and 56 of title 21 Code of Federal Regulations.

The ANPRM's proposals on volume bulk thresholds affect three categories of data that, in the normal course of biopharmaceutical firms' global clinical research programs, are routinely used, collected, processed, disclosed, and maintained, namely: human genomic data, biometric identifiers, and personal health data.

The U.S. is home to many of the world's most cutting-edge and innovative biotech companies, laboratories, research centers, and hospitals. As a result, patients in the U.S. have access to the most innovative therapeutics and cutting-edge clinical studies in the world. Accordingly, data on U.S. individuals constitute a significant percentage of the participants in global clinical research programs and, as a consequence, a significant percentage of the data companies rely on when seeking marketing authorization for the approval of their drugs at the FDA and abroad constitutes data originating from U.S. individuals.

Typically, clinical studies involve hundreds of patients and regulatory filings may rely on multiple studies. For example, most vaccine registration studies include tens of thousands of study participants. Accordingly, data on U.S. individuals, over the course of a 12-month period, used, collected, processed, or disclosed by biopharmaceutical firms will likely exceed the minimum thresholds envisioned in the proposed rules for genomic (100 individuals), biometric (100 individuals), or personal health data (1,000 individuals).

In the course of a global, multi-regional clinical research program, data will also routinely be transferred to employees, research partners and collaborators to assess and study trial data. This scientific analysis may from time to time involve transfers to "covered persons" or to "countries of concern," particularly in the case when studies are also being conducted in countries of concern.

In addition to the transfers of data as part of global clinical trial and research programs, biotech firms may transfer data to regulatory authorities in countries of concern to substantiate claims of safety, efficacy, and quality of their drugs as part of an effort to obtain marketing authorization and regulatory approval so that innovative treatments may be made available to patients in countries of concern. As aforementioned, regulatory filings may require transfers of data of multiple clinical studies, including genomic, biometric, and personal health data, of U.S. individuals.

Under ICH GCPs, all clinical trial data must be verifiable against the underlying patient medical records to ensure the data are accurate. Under this standard, the FDA can inspect clinical trial sites around the world, including in countries of concern, and other global regulatory authorities can do

the same in the United States. Given the quantity of data required and the number of U.S. individuals typically involved in cutting-edge global therapeutic clinical study programs, transfers for regulatory approval will likely exceed bulk volume thresholds currently under consideration.

Finally, clinical research and filings for drug authorization are not the only instances when transfers of data may be impacted. The international transfer of data on U.S. individuals is also critical for other public health activities, such as those set forth in section 164.512 of title 45 of the Code of Federal Regulations and other equivalent foreign laws and regulations, where companies must report pharmacovigilance data and adverse events related to their product.

As clinical trials are run on a small percentage of patients compared to the real-world setting, after a new drug is approved, biopharmaceutical companies are required to monitor for additional side effects and other issues related to the approved drug. All such data, no matter where in the world the patient is, must be reported to all regulators where the trial was run and where the drug received marketing authorization. Data are normally submitted in pseudonymized or aggregate form, but for certain high-risk incidents (e.g., drug related death), individual reporting may be required. Regulatory authorities may also ask for copies of records to better understand the circumstances around such severe cases. The same data is reported globally for those regulators who have implemented ICH guidelines. Such monitoring and reporting are required over the lifetime of the drug. For a biopharmaceutical company with multiple approved drugs, a company could easily reach the caps on the bulk transfer of health data, especially as this would be in addition to the clinical trial data that is being reported.

All safety and efficacy data that is collected as part of the trial and all documentation related to the trial must be submitted to all regulatory authorities in countries where the trials are run and where marketing authorization is sought. Therefore, all regulatory authorities receive the same information to review the safety and efficacy of the medication. Sharing of patient safety data, therefore, benefits U.S. citizens and patients living in the U.S. and elsewhere. The proposals in the ANPRM pose risks to this globally harmonized system and if implemented may delay new medicines from reaching the market.

Accordingly, biopharmaceutical firms may exceed minimum bulk volume thresholds proposed in the rules and, thus, potentially risk engaging in prohibited bulk volume transfers of sensitive personal data of U.S. individuals, as a result of conducting innovative global clinical research programs or by seeking drug approvals in countries of concern.

Comments re: anonymization, pseudonymization, and de-identification

The proposed rules treat data that is anonymized, pseudonymized, de-identified, and encrypted equally to data that is personally identifiable information. BIO does not believe that the calculus for bulk volume thresholds for anonymized, pseudonymized, de-identified, and encrypted data should be the same as the calculus for bulk volume thresholds of personally identifiable information.

Although reidentification of data is, in theory, a possibility, the volume thresholds should be more carefully calibrated to account for the scientific community and industry's ability to anonymize, pseudonymize, and de-identify data sets in a manner that preserves the scientific integrity of research data, promotes legitimate national security concerns, and that appropriately safeguards U.S. individuals' privacy rights.

For example, the genomic, biometric, and personal health data on U.S. individuals biopharmaceutical firms routinely use, collect, process, disclose, and maintain in the course of research and development efforts are pseudonymized or de-identified in accordance with the requirements for de-identification set forth in section 164.514 of title 45 of the Code of Federal Regulations and are derived from individually identifiable health information, as described in the Health Insurance Portability and Accountability Act of 1996, or personal information, consistent with the Federal Policy for the Protection of Human Subjects or the human subject protection requirements of the FDA.

If the proposed bulk volume thresholds for anonymized, pseudonymized, and de-identified data were the same as the thresholds for personally identifiable information, innovative biotech firms in the U.S. will, in the natural course of their research and commercial efforts, quickly exceed minimum bulk volume thresholds proposed in the rules.

BIO also encourages the DOJ to consider how privacy enhancing technologies could potentially be incorporated into the definition of bulk volume thresholds in such a way that privacy enhancing tools promote legitimate national security concerns associated with transfers of data to countries of concern and covered persons while also allowing for the transfer of this data to accelerate and drive cutting-edge biopharmaceutical research efforts in the United States.

Comments re: covered data transactions

BIO acknowledges the DOJ's efforts to carefully tailor the proposed rules to achieve the Executive Order's intent and effect; however, the definition of covered data transaction is overly broad, particularly the definitions of *data brokerage* and *vendor agreement:*

> *A covered data transaction is any transaction that involves any bulk U.S. sensitive personal data or government-related data and that involves: (1) data brokerage; (2) a vendor agreement; (3) an employment agreement; or (4) an investment agreement.*

Given the likelihood for biotech firms to exceed bulk U.S. sensitive personal data thresholds as described above, biotech firms' engagement in "covered data transactions" under the proposed rules would depend on the extent to which a data brokerage, vendor agreement, employment agreement or investment agreement are involved in a transaction.

With respect to the definition provided for data brokerage, and aside from Examples 16-18 provided in the ANPRM, the proposed definition could implicate the involvement of a data brokerage in scenarios where biotech firms transfer bulk U.S. sensitive personal data in de-identified form to research collaborators in a covered country. Additionally, it could impact scenarios where biotech firms transfer bulk U.S. sensitive personal data in pseudonymized or de-identified form to a regulatory authority in a country of concern as part of a regulatory filing to seek marketing approval of a new therapeutic.

The terms "sale of, licensing of access to, or similar commercial transactions" could encompass a broad range of meaningful and routine transactions of data. Indeed, the term "transaction" as defined in the ANPRM applies broadly to any use, transfer, or holding of data.

Similarly, the definition for *vendor agreement* presents concern given its broad scope which would encompass any agreement or arrangement, in which any person provides goods or services to another person in exchange for consideration. In addition to those vendor agreements illustrated in Examples 19-22 of the ANPRM, we note that there are many other arrangements critical to the scientific process that may be captured as a vendor agreement, resulting in the potential significant disruption of global scientific collaborations.

Accordingly, a considerable amount and variety of data transfers could be categorized as involving a *data brokerage* or *vendor agreement*. Therefore, assuming bulk volume thresholds of U.S. sensitive personal data are met, even if the data is in de-identified or anonymized form, scientifically relevant transfers of data needed to drive biomedical research and development or to ensure new therapies reach patients around the world could qualify as covered data transactions under the proposed rules.

Outcomes significantly disrupting global scientific collaborations and the delivery of breakthrough treatments to patients around the world seem to run counter to the DOJ's stated assertion that "[this ANPRM does not] seek to broadly prohibit U.S. persons from conducting commercial transactions with entities and individuals located in countries of concern or impose measures aimed at a broader decoupling of the substantial consumer, economic, scientific, and trade relationships that the United States has with other countries."

Given this potential broad scope and ramifications for the innovative U.S.-based biopharmaceutical sector, BIO welcomes the opportunity to work with the DOJ to further tailor and clarify key definitions in order to more clearly describe the transactions intended to be covered.

Comments re: prohibited covered data transactions

Aside from the examples provided in the ANPRM, routine transfers of scientifically-relevant data could fall within scope of the proposed prohibited covered data transactions, despite efforts to develop tailored and targeted rules.

As noted above, biotech firms in the normal course of their business and research exercises may exceed bulk volume thresholds and the transfers of scientifically-relevant bulk sensitive personal data to drive biopharmaceutical R&D efforts or to obtain a marketing approval with a government regulatory agency may be classified as covered data transactions involving a data brokerage or a vendor agreement and thus fall under the definition of a prohibited covered data transaction. This outcome seems to be the case whether U.S.-based biotechnology companies were dealing with personally identifiable information or whether they were dealing, as is customary, with anonymized, pseudonymized, or de-identified information.

Comments re: exemptions for regulatory-compliance related transactions

Given the potential for the proposed rules to encompass a significant range of data transfers relevant to U.S.-based biotech firms' research and commercial operations, BIO proposes for consideration exemptions that, in combination with additional safeguards, may achieve the overall objectives of the Executive Order and provide robust protections of U.S. individuals' sensitive personal data.

First, it may be helpful to consider an exemption for companies to submit data as part of a regulatory submission to government regulatory bodies in order to obtain licensure to lawfully provide and distribute drugs to patients in countries of concern.

In addition, as it stands, the proposals included in this ANPRM would apply equally to personally identifiable information as they would to anonymized, pseudonymized, or de-identified data. BIO encourages the DOJ to consider tailoring the rules for data transfers involving anonymized, pseudonymized, de-identified, encrypted, or otherwise privacy-protected data. Furthermore, BIO encourages the DOJ to consider how the use of privacy enhancing technologies may support permissible transfers of data to drive biomedical research and delivery of treatments to patients abroad.

BIO also seeks clarification on Example 49 regarding an exemption permitting a scenario where a U.S. hospital conducting genomic research on U.S. persons may contract with a foreign laboratory and employ a researcher who is a covered person when these contracts are part of federally funded research. We welcome feedback and rationale from the DOJ that would permit this transfer when federal funds, as opposed to private funds, are being used to fund the research project.

Finally, the exemptions for regulatory compliance provided in this ANPRM seem to be entirely oriented around financial regulations and we would welcome the opportunity to work with the DOJ to explore additional exemptions that help to promote and preserve U.S. innovation and leadership in the life sciences while also addressing legitimate national security concerns raised in the ANPRM. We believe exemptions, in contrast to potential licensing tools modeled on the regime used by OFAC as envisioned in this ANPRM, could contribute to a more efficient framework that enables continued U.S. leadership in the research, development, and delivery of breakthrough biomedical technologies for patients around the world.

Conclusion

As aforementioned, biotechnology is a national security imperative for BIO. We support the Executive Order and the development of tailored rules surrounding international transfers of Americans' bulk sensitive personal data to strengthen our national security and protect the exploitation of data by countries of concern. We also, however, believe that U.S. leadership in the life sciences is a critical element of a robust and comprehensive national security plan and future rules, therefore, must carefully balance these considerations.

The proposals in this ANPRM are an important step forward. BIO appreciates the DOJ's efforts to carefully consider rules and calibrate actions that minimize risks and disruptions to the U.S.-based innovative biopharmaceutical sector and we look forward to further collaborations on this topic.

About BIO

BIO is a non-profit organization based in Washington, D.C. with a membership of more than 1,000 biotechnology companies throughout the United States. BIO's members research and develop innovative health care, agricultural, industrial, and environmental biotechnology products. Over 90% of BIO's members are small and medium sized enterprises, many of whom are still pre-commercial.