hrp CONSULTING GROUP
Research Ethics & Compliance Solutions
Tel: 347.862.9321
info@thehrpconsultinggroup.com
thehrpconsultinggroup.com

Preventing Access to Sensitive US Data by Countries of Concern: DOJ Rule & NIH Policy

This document outlines rules from the Department of Justice (DOJ) and the National Institutes of Health (NIH) regarding access to sensitive U.S. personal data by "countries of concern" (identified as China, Russia, Iran, North Korea, Cuba, and Venezuela).

The Department of Justice (DOJ) issued a Final Rule to implement Executive Order 14117, aiming to prevent access to Americans' bulk sensitive personal data and U.S. government-related data by countries of concern (China, Russia, Iran, North Korea, Cuba, and Venezuela) and covered persons with ties to those countries. This rule restricts U.S. persons from engaging in certain data transactions involving such data with these entities, identifying classes of prohibited and restricted transactions. The DOJ's goal is to address national security risks posed by the potential exploitation of this data by foreign adversaries. The rule became effective on April 8, 2025.

NIH issued an Implementation Update on April 4, 2025, to enhance the security of controlled-access data by prohibiting access by institutions located in the same countries of concern.

DOJ Final Rule Exemptions for Research

The DOJ Final Rule restricts access to Americans' bulk sensitive personal data but includes several exemptions relevant to research:

1. **Official Business of the U.S. Government**:
    - Exempts data transactions under federal grants, contracts, or agreements (e.g., NIH, NSF, DOD funding).
    - Caveat: Institutions still require due diligence and documentation; DOJ retains audit authority. This exemption does not override other rules like NIH access policies.
2. **Information or Informational Materials**:
    - Exempts transactions involving expressive materials (videos, artwork, publications) under 50 U.S.C. § 1702(b)(3).
    - Excludes technical or functional data.
    - Includes associated metadata necessary for transmission.
3. **Drug, Biological Product, and Medical Device Data**:
    - Exempts data transactions necessary for regulatory authorization/approval (e.g., FDA submissions, clinical investigations, post-marketing surveillance).

Tel: 347.862.9321
info@thehrpconsultinggroup.com
thehrpconsultinggroup.com

- Applies if data is de-identified or pseudonymized and recordkeeping requirements are met.
- Includes human 'omic data.

4. **International Agreements**:
   - Exempts transactions required/authorized by federal law or international agreements (e.g., global health data sharing).
5. **Publicly Available Data**:
   - Excludes data lawfully available from government records or widely distributed media, including open-access repositories.

Key DOJ Rule Points

1. **Focuses on commercial transactions** involving payment or valuable consideration.
   - In the context of research under the new DOJ regulations, a commercial transaction generally involves payment or other valuable consideration for access to or transfer of data. This includes activities such as:
     - Data brokerage: sale or licensing of bulk U.S. sensitive personal data to a country of concern or covered person.
     - Vendor agreements: U.S. persons contracting with a covered person for payment and providing access to covered data, like hiring a foreign lab for payment and providing biospecimens and genomic data.
     - Employment agreements: U.S. persons employing a covered person with access to covered data.
     - Investment agreements: covered persons gaining ownership interest that provides access to covered data.
   - Conversely, activities that are generally NOT commercial transactions in research typically do not involve an exchange of payment or other valuable consideration. This includes:
     - Research collaborations without an exchange of payment or other valuable consideration. Mutual interest in research or potential co-authorship generally does not qualify as "valuable consideration".
     - U.S. research in countries of concern or partnerships that do not involve a prohibited commercial transaction.
2. **Research collaborations without such commercial exchange might not be covered.**
3. The rule **does not prohibit** U.S. research in countries of concern or collaborations with

Tel: 347.862.9321
info@thehrpconsultinggroup.com
thehrpconsultinggroup.com

them, **unless a prohibited/restricted commercial transaction is involved.**

NIH Policy (NOT-OD-25-083) - Additional Restrictions

The NIH issued notice NOT-OD-25-083 (effective date April 4, 2025) which imposes restrictions independent of the DOJ rule:

- **Prohibition**: Institutions located in countries of concern are prohibited from accessing NIH Controlled-Access Data Repositories.
- **Overrides DOJ Exemptions**: This NIH prohibition applies even if the transaction would be exempt under the DOJ's "official business" (federal funding) rule.
- **Caution Advised**: Review services/collaborations involving vendors or institutions with ties to countries of concern carefully, as they may trigger NIH restrictions or other risks, even if DOJ-exempt.

Interaction and Key Considerations

- **Compliance with Both**: Institutions must comply with both DOJ regulations and NIH policies.
- **DOJ Exemption ≠ NIH Override**: A DOJ exemption (e.g., for federal funding) does not negate NIH's specific access restrictions for its controlled-access data.
- **Due Diligence**: Regardless of exemptions, thorough due diligence and documentation are crucial.

Breakdown of the Interaction of the Rule and Policy

Summary: While the DOJ rule offers certain research-related exemptions, the NIH policy imposes an additional layer of restriction specifically concerning access to NIH-controlled data by institutions in countries of concern. Even if a research activity is exempt under the DOJ rule (e.g., due to federal funding), the NIH can still prohibit access to its controlled-access data repositories by institutions in the listed countries. Institutions involved in NIH-funded research with controlled-access data must therefore navigate both sets of regulations to ensure compliance.

- **DOJ Exemption for Federally Funded Research**: The DOJ Final Rule provides an exemption for data transactions conducted under the official business of the U.S. government, including those carried out under federal grants, contracts, or agreements. Federally funded

Tel: 347.862.9321
info@thehrpconsultinggroup.com
thehrpconsultinggroup.com

research involving access by a covered person or entity may be exempt from the DOJ's restrictions if the transaction falls within the scope of that federal funding.

- **NIH Prohibition on Access**: The NIH policy specifically prohibits institutions located in countries of concern (China, Russia, Iran, North Korea, Cuba, and Venezuela) from accessing NIH Controlled-Access Data Repositories. This prohibition applies regardless of whether the transaction is federally funded or would otherwise be exempt under the DOJ rule.

- **Parallel Compliance Obligation**: The NIH policy creates a parallel compliance obligation. Even if a federally funded research project involving data transfer to a covered person in a country of concern qualifies for the DOJ's "official business" exemption, the NIH policy still bars institutions in those countries from accessing NIH Controlled-Access Data Repositories.

- **DOJ Exemption Does Not Override NIH**: The DOJ rule explicitly notes that its exemptions do not override other agency-specific rules, such as the NIH access policies. Therefore, a DOJ exemption for federally funded research does not negate the NIH's access restrictions. Institutions must comply with both sets of requirements.

- **Focus on NIH Data Repositories**: The NIH policy is specifically focused on controlling access to its Controlled-Access Data Repositories by institutions in countries of concern.

Conclusion: While the DOJ rule offers research-related exemptions, the NIH policy specifically bars institutions in countries of concern from accessing NIH Controlled-Access Data Repositories. Institutions managing NIH-funded research with controlled-access data must carefully evaluate both sets of rules.

Tel: 347.862.9321
info@thehrpconsultinggroup.com
thehrpconsultinggroup.com

Resources

- **DOJ Final Rule** - Federal Register: https://www.federalregister.gov/d/2024-31486. This is the official publication of the final rule titled "Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons." It contains the complete legal text of the regulations.
- **DOJ Data Security Program: Implementation and Enforcement Policy Through July 8, 2025:** https://www.justice.gov/opa/media/1396346/dl?inline. Addresses enforcement of the Rule, including key compliance dates and a 90-day enforcement discretion period during which DOJ will not prioritize civil enforcement actions as long as good faith efforts are being made to come into compliance. However, enforcement action may be taken during this period if there are egregious, willful violations.
- **DOJ Data Security Program: Frequently Asked Questions:** https://www.justice.gov/opa/media/1396351/dl. Provides clarification regarding several aspects of the rule, including when the rule does or does not apply to research activities.
- **National Security Division (NSD) Website** - U.S. Department of Justice: https://www.justice.gov/nsd. This is the official website of the DOJ's National Security Division, which is responsible for implementing and enforcing the final rule. It is a primary source for information and potential future guidance.
- **DOJ Press Release (April 11, 2025)**: https://www.justice.gov/opa/media/1396351/dl. This is an official press release from the DOJ providing a summary and explanation of the final rule, including definitions of key terms like "data brokerage" and "sensitive personal data".
- **NIH Notice NOT-OD-25-083**: Implementation Update: Enhancing Security Measures for NIH Controlled-Access Data. This notice, released on April 2, 2025, outlines the NIH's implementation of enhanced security measures for NIH Controlled-Access Data Repositories. https://grants.nih.gov/grants/guide/notice-files/NOT-OD-25-083.html
- **NIH Security Best Practices for Controlled-Access Data and Repositories:** https://sharing.nih.gov/accessing-data/NIH-security-best-practices. Describes NIH's expectations for users of controlled-access data, repositories that store such data, and NIH systems that provide access to such data. Includes a list of controlled-access repositories that are implementing NIH Security Best Practices.