UNIVERSITY OF CALIFORNIA

Research Policy Analysis & Coordination

Guidance Memo **25-04**

November 13, 2025

To: Contracting Office Directors
Contracts & Grants Officers
Research Compliance Offices

Subject: Guidance on the DOJ Bulk Data Rule and Compliance in Research Contracting

Purpose:

This Guidance is intended to help all campus units and personnel involved in research contracting and compliance understand and comply with the Department of Justice's Final Rule at 28 CFR Part 202 titled *Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons* ("DOJ Bulk Data Rule").

The DOJ Bulk Data Rule is broad and applies to many types of transactions. Although this Guidance is geared towards research contracting scenarios, it may also apply to other scenarios. Non-research related scenarios arising under the DOJ Bulk Data Rule, such as transactions involving financial data, are not addressed in this Guidance, but may be managed by local campuses. This Guidance should be read broadly to apply to nontraditional research contracting scenarios, such as nonmonetary transactions with an exchange of consideration (e.g., mutual sharing of datasets between parties).[1]

Guidance:

1. **Overview of the DOJ Bulk Data Rule.**

The DOJ Bulk Data Rule restricts certain types of data transactions involving sensitive U.S. personal and government-related data. It applies to any U.S. institution that may transfer such data to foreign persons or entities, particularly those associated with countries of concern. The DOJ Bulk Data Rule is broad and applies to both commercial and non-commercial transactions, including research collaborations. Research offices should be aware that this includes:

- Any agreement where data is shared, accessed, stored, or transferred.
- Transactions involving foreign collaborators, subcontractors, or data recipients.
- Situations where data may be aggregated over time to meet bulk thresholds.

[1] *FACT SHEET: Justice Department Issues Final Rule to Address Urgent National Security Risks Posed by Access to U.S. Sensitive Personal and Government-Related Data from Countries of Concern and Covered Persons (PDF)*, page 10.

Pursuant to the DOJ Bulk Data Rule, UC **cannot knowingly share or provide access** to defined bulk U.S. sensitive personal data or certain government-related data with **covered persons unless a specific exemption applies. Additionally,** when transferring or giving access to such data to any **non-covered foreign persons or entities**, UC must include **contractual terms** prohibiting that party from allowing subsequent access to that data to a covered person or country of concern. The Guidance provides template contractual terms in order to prevent the onward transmittal of bulk sensitive or government-related data to covered persons.

2. Key Definitions.

The DOJ Bulk Data Rule defines several key terms relevant to compliance. RPAC included simplified reference definitions below; the regulatory definitions appear in §§ 202.201-202.259.

- **Bulk U.S. Sensitive Personal Data**: Large datasets containing information such as personal health (>10,000 U.S. persons), financial (>10,000 U.S. persons), biometric identifies (>1,000 U.S. persons), genetic data (>1,000 U.S. persons), and genomic data (>100 U.S. persons) regardless of whether the data is anonymized, pseudonymized, de-identified, or encrypted.[2]
- **Government-Related Data**: Specific information related to particular U.S. government operations or personnel.
- **Covered Person**: Certain foreign persons or entities associated with a country of concern.
- **Countries of Concern**: **China, Cuba, Iran, North Korea, Russia, Venezuela**
- **Data Brokerage**: Any commercial transaction involving the sale, licensing, or exchange of data for value.

3. Assessing DOJ Bulk Data Rule Compliance for Outgoing Contracts.

For outgoing contracts where the other party is a covered person, the campus may not engage in a covered data transaction involving data brokerage unless an exemption applies.

Where the other party is not a covered person, the DOJ Bulk Data Rule broadly requires U.S. institutions to ***affirmatively*** act to contractually prohibit onward transfers of bulk U.S. sensitive personal data or government-related data to covered persons as defined and described under the Rule when outwardly transferring that data and any foreign person may have access to that data. To comply with the affirmative obligation, campus contracting offices have two options to ensure outgoing contracts are compliant.

The first approach is for the contracting office to review ***each*** outgoing contract individually to decide whether it needs to include DOJ Bulk Data Rule contractual terms. The second approach is to include the compliance terms in ***all*** outgoing contracts by default.

Under the first approach, campus offices must carefully evaluate each outgoing contract to determine whether it triggers compliance obligations under the DOJ Bulk Data Rule. Specifically, offices should assess whether the transaction involves:

[2] The thresholds for the datasets are computed on an aggregated, ongoing 12-month basis per campus. For example, if a campus has two contracts with Company X and each involve 7,500 personal health records, the Rule would apply to the transactions even though the Rule wouldn't be triggered until the latter contract is effective.

- **Data Brokerage**: This includes selling, licensing, or exchanging data for any form of value in a commercial transaction. In an individualized collaborative context, individual researchers sharing datasets in return for access to other data, tools, or collaborative results is generally exempt from the Rule.[3]
- **Foreign Access**: There is a likelihood a foreign person, entity, or government will receive access to specified government-related data or bulk U.S. personal data. Indicators of whether there will be foreign access include:
    - A non-U.S. citizen or lawful resident will have access the data while they are not physically within the U.S.
    - The other party is an entity based outside the U.S.
    - The other party is owned or controlled by a foreign entity.
    - The data recipient is a foreign researcher or institution.
- **Sensitive Data Access**: The contract allows access to bulk U.S. sensitive personal data or government-related data.
- **Non-Covered Persons**: The foreign party is not classified as a "covered person" under the Rule.
- **No Applicable Exemptions**: The transaction does not fall under an exemption. The most common exemptions[4] UC will encounter are transactions that involve:
    - "official business of the U.S. government" (i.e., transactions for activities fully funded by the federal government, including for federal research grants and contracts);
    - "drug, biological product, and medical device authorizations"; and
    - "other clinical investigations and post-marketing surveillance data."

If the assessed outgoing contract meets ***each*** of the prerequisites above, then the campus contracting office ***must*** use contract terms to prohibit onward transfers of bulk sensitive or government-related data to covered persons. See Appendix A for template contract terms. As a best practice, and as shown in Appendix A, contract terms must require the other party to report any known or suspected access violations to the local campus immediately.

Following the second approach, where the contracting office includes confirmatory language in ***all*** outgoing contracts, the contracting office will ***still*** need to assess whether the other party is a "covered person" under the Rule before inserting the confirmatory language. If the other party is not a covered person, the contracting office can use the template language provided in Appendix B.

4. Reviewing Incoming Research-Related Agreements.

Incoming agreements may include clauses requiring the campus comply with the DOJ Bulk Data Rule. Contracting offices should:

[3] See Example 9 at § 202.214.

[4] Exemptions found at § 202.402.

- **Assess exemptions** to determine if the DOJ Bulk Data Rule applies. Common exemptions include federally funded research, clinical investigations, and government-authorized medical product data.
- **Request confirmation** from the data provider regarding DOJ Bulk Data Rule applicability. If the provider cannot confirm, the campus should avoid accepting obligations that may trigger compliance requirements.[5]
- **Consider potential additional transactions** to determine if the contemplated engagement also involves onward data transactions. This may include collaborations with multiple parties involving outgoing data sharing; outgoing subcontracts; and making data available to consortium members including by repositories.
- **Avoid accepting obligations** without clarity on data volume or type. If the agreement lacks specificity, seek clarification or propose revised language.
- **Notify relevant campus parties**, including Principal Investigators, of any restrictions or obligations imposed by the Rule.

5. Reporting Obligations.

§ 202.302(b) requires a report of any known or suspected violations of the prohibitions on onward transfer of data to the federal Department of Justice ***within 14 days*** of the violation becoming known or suspected. Campuses are recommended to develop local business processes with relevant campus departments to manage the reporting compliance obligations. It is the responsibility of the local campus to report violations to the Department of Justice.

6. Recordkeeping.

The DOJ Bulk Data Rule requires a "full and accurate record" of each transaction subject to the Rule to be maintained for a period of 10 years.[6] The 10-year retention period may exceed UC's standard retention schedule for such transactions. The DOJ Bulk Data Rule does not define what constitutes a "full and accurate record". It is advisable to keep copies of all executed contract documents, logs, reports, relevant correspondence, and any institutional policies in effect at the time of contracting for any transaction subject to the Rule.

7. Intracampus Collaboration to Maintain Compliance.

Since Bulk Data thresholds can be met by aggregating total records transferred across multiple transactions in a 12-month period, campuses should develop procedures to track otherwise-qualifying transactions that do not meet the bulk thresholds to know when DOJ Bulk Data Rule compliance will be triggered. These transactions may arise from contracts managed by different local campus contracting offices.

Campuses should identify or establish a local coordinating office or cross-functional team to track and monitor applicable transactions to ensure Rule compliance.

---

[5] See *The Negotiator's Handbook* entry on the DOJ Bulk Data Rule for examples of language to include in incoming contracts to ensure the other party confirms Rule applicability.

[6] § 202.101

At this time, UCOP's understanding is that the Rule applies on a campus-by-campus basis, not collectively on a systemwide basis, meaning transactions only need to be aggregated at local campuses, not across the UC system. An example is provided to illustrate why campuses need to develop procedures to track otherwise-qualifying transactions that do not meet the bulk thresholds.

> ***Example:*** A campus Department of Internal Medicine engages ACME, a foreign entity qualifying as a covered person under the Rule, to perform services under a business contract handled by the campus's Business Contracts Office. The campus intends to send 9,000 records of Personal Health Data to ACME, so that transaction alone does not qualify as a "covered data transaction" under the Rule. However, 4 months prior, the campus's Department of Ophthalmology engaged ACME as a subcontractor on a sponsored research agreement through the Sponsored Research Office, and sent 5,000 records of Personal Health Data to ACME. The prior transaction from Ophthalmology would not have triggered the Rule's prohibitions, but the latter transaction for Internal Medicine would be prohibited because it would cause ACME to receive more than 10,000 records of Personal Health Data from the campus within a 12-month period.

Each campus has multiple contracting offices subject to distinct organizational reporting requirements. It is imperative that each campus develop a cross-functional approach to centrally track otherwise-qualifying transactions would be prohibited by the DOJ Bulk Data Rule but for the transaction not meeting the bulk quantity thresholds.

Contact

Brian Russ
Brian.Russ@ucop.edu

Agnes Balla

Agnes Balla
Director
Research Policy Analysis & Coordination

Appendix A – Sample Contract Terms for § 202.302(a)(1) Compliance

[where applicability confirmed]

*Applicability: This clause is provided as a sample of what to use in outgoing subcontracts (but can be revised for other types of agreements) where the campus contracting office **determines** the agreement is subject to the onward data transfer prohibitions of 28 CFR § 202.302(a)(1).*

Data Transfer Restrictions and Compliance (28 CFR § 202.302(a)(1))

1. Definitions. For the purposes of this Section, the following definitions apply as defined in 28 CFR Part 202: "Bulk U.S. Sensitive Personal Data," "Country of Concern," "Covered Data Transaction," "Covered Person," "Data Brokerage," and "Government-Related Data."

2. Prohibition on Onward Transfer. Subcontractor [*Note: or other entity name as defined in applicable agreement*] acknowledges that any data provided by University to Subcontractor to use, store, or access pursuant to this Subcontract [*Note: or other agreement-defined term*] constitutes "Bulk U.S. Sensitive Personal Data" or "Government-Related Data," and is subject to federal regulations concerning data access by countries of concern or covered persons.

Subcontractor agrees that it shall not engage in a subsequent Covered Data Transaction involving Data Brokerage of the same data received under this Subcontract with any Country of Concern or Covered Person.

3. Reporting Obligations. Subcontractor agrees to report any known or suspected violations of the contractual prohibition outlined above (in Prohibition on Onward Transfer) to University within seven (7) days of becoming aware of or suspecting such violation. University reserves the right to report such violations to the U.S. Department of Justice in accordance with 28 CFR § 202.302(b).

4. Breach. Subcontractor shall be responsible for any and all claims, liabilities, penalties, fines, or damages against University arising out of Subcontractor's failure to comply with 28 CFR § 202. Failure to comply with the provisions of this Section shall constitute a material breach of this Subcontract.

Appendix B – Sample Contract Terms for § 202.302(a)(1) Compliance

[where applicability presumed]

*Applicability: This clause is provided as a sample of what to use in outgoing subcontracts (but can be revised for other types of agreements) where the campus contracting office **presumes** the agreement is subject to the onward data transfer prohibitions of 28 CFR § 202.302(a)(1) after confirming the other party is not a covered person.*

Data Transfer Restrictions and Compliance (28 CFR § 202.302(a)(1))

1. Definitions. For the purposes of this Section, the following definitions apply as defined in 28 CFR Part 202: "Bulk U.S. Sensitive Personal Data," "Country of Concern," "Covered Data Transaction," "Covered Person," "Data Brokerage," and "Government-Related Data."

2. Prohibition on Onward Transfer. Subcontractor [*Note: or other entity name as defined in applicable agreement*] acknowledges that any data provided by University to Subcontractor to store, use, or access pursuant to this Subcontract [*Note: or other agreement-defined term*] may constitute "Bulk U.S. Sensitive Personal Data" or "Government-Related Data," and may alone or in aggregate with data provided to Subcontractor under prior or subsequent agreements, become subject to federal regulations concerning data access by countries of concern or covered persons.

Subcontractor agrees that it shall not engage in a subsequent Covered Data Transaction involving Data Brokerage of the data received under this Subcontract which is "Bulk U.S. Sensitive Personal Data" or "Government-Related Data" with any Country of Concern or Covered Person.

Notwithstanding any ambiguity or uncertainty regarding whether the volume, nature, or specific characteristics of the data received, processed, or accessed by the Subcontractor definitively meet the precise thresholds or definitions for direct regulatory applicability of 28 CFR 202 (or any successor regulation), the Subcontractor hereby unconditionally agrees to comply with all requirements set forth in 28 CFR 202 or later flowed down by the University. This includes, but is not limited to, adherence to all provisions concerning the security, privacy, dissemination, and audit of such data, and the establishment and maintenance of a comprehensive security and privacy program specifically tailored for data operations that may be subject to this rule.

3. Reporting Obligations. Subcontractor agrees to report any known or suspected violations of the contractual prohibition outlined above (in Prohibition on Onward Transfer) to University within seven (7) days of becoming aware of or suspecting such violation. University reserves the right to report such violations to the U.S. Department of Justice in accordance with 28 CFR § 202.

4. Breach. Subcontractor shall be responsible for any and all claims, liabilities, penalties, fines, or damages against University arising out of Subcontractor's failure to comply with 28 CFR § 202. Failure to comply with the provisions of this Section shall constitute a material breach of this Subcontract.

Appendix C – Decision Tree to Assess Rules Applicability

The following decision tree is provided to aide campuses in determining if the DOJ Bulk Data Rule applies to a given transaction. The decision tree is a simplified assessment and shouldn't be considered a comprehensive analysis.

Decision Tree to Assess if the DOJ Bulk Data Rule Applies to the Transaction:

1. **Does the transaction involve data?**
    a. If no, the Rule does not apply.
    b. If yes, go to Question #2.
2. **Does the data involved constitute bulk U.S. sensitive personal data (either alone or in aggregate with other transactions with the same other party within the past 12 months) or government-related data as defined by the Rule?**
    a. If no, the Rule does not apply.
    b. If yes, go to Question #3.
3. **Is the other party foreign?**
    a. If no, the Rule does not apply.
    b. If yes, go to Question #4.
4. **Does the transaction qualify as data brokerage?**
    a. If no, the Rule does not apply.
    b. If yes, go to Question #5.
5. **Is the transaction exempt from the Rule?**
    a. If yes, the Rule does not apply.
    b. If no, the Rule applies.