COMPLIANCE ALERT FEBRUARY 2026

COMPLIANCE WITH THE DEPARTMENT OF JUSTICE BULK DATA RULE

KEY TAKE AWAY

The DOJ's new rule[1] (Final Rule) **may** limit or require federal authorization *before* large amounts of **sensitive data** are shared with **foreign institutions, collaborators, vendors, or cloud services.** In a university setting, "bulk data transfers" can occur during routine activities—such as sharing large research datasets with international collaborators, storing data on overseas servers, or using foreign-based data processing services. Because UC conducts extensive international research and routinely exchanges data across borders, failing to follow the rule could create significant compliance and legal risks.

Who Is Impacted

- Compliance officers (CECOs, research compliance, export control teams)
- Procurement staff
- Sponsored Programs Offices or other central administrative offices involved in negotiation of research or research-related agreements
- IT/security/data governance staff
- **Researchers and PIs who share or transfer research datasets internationally**

Background

The Final Rule, which took effect on October 6, 2025, restricts certain commercial data transactions involving: bulk U.S. sensitive personal data, and U.S. government-related data when data is accessed by, transferred to, or otherwise made available to countries of concern or a covered person, including through UC research, vendor, or data sharing agreements.

In practice, campuses must:

- ✓ Understand when research data, biospecimens, 'omic data, or datasets meet the Rule's volume or category thresholds.
- ✓ Identify when foreign collaborators, vendors, researchers, or subcontractors may be "covered persons" or associated with countries of concern – i.e. China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia, Venezuela.
- ✓ Evaluate transactions for potential foreign access to sensitive or government-related data.

The Final Rule applies whether data is anonymized, pseudonymized, de-identified, or encrypted. Thresholds are based on all data *aggregated* across campus transactions in a rolling 12-month period to the same recipient, meaning small transactions may collectively trigger compliance requirements.

What Are My Compliance Obligations?

Because data thresholds are *aggregated* across a campus,[2] each campus must:

- ✓ Track data transfers, even those below the set thresholds, across the campus

Campuses should also:

[1] Federal Register :: Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons

[2] This applies if a campus permits covered data to be accessed by, transferred to, or otherwise made available to countries of concern or covered persons.

- ✓ Include DOJ-required contractual protections in agreements involving foreign access to covered data, including language to prevent onward transfer of data by a foreign entity in a non-country of concern[3]
- ✓ Report all known or suspected violations of the contractual prohibition on onward transfer to a country of concern by a foreign entity to the Department of Justice within 14 days
- ✓ Ensure access to covered data is terminated in a timely manner following separation from a campus
- ✓ Establish a program to:
  - Ensure covered data is stored and accessed only through university-managed systems subject to campus procedures
  - Maintain 10-year records for covered transactions, prohibited, restricted, and some exempt transactions[4]
  - Conduct an annual audit of restricted transactions, records, and security controls[5]
  - Implement a data compliance program[6] for restricted transactions that, among other requirements, include risk-based procedures for verifying data flows in an auditable manner, procedures for verifying the identity of vendors, and written policies describing the data compliance program *and* implementation of the security requirements[7] – both of which are annually certified by an officer, executive or other employee responsible for compliance
- ✓ Report rejected prohibited transactions to the Department of Justice within 14 business days of rejecting it

Indicators Data May Fall Under the Rule

Any of the following may trigger the need for compliance with the Final Rule:

- ✓ Large datasets or biospecimens involving these thresholds:
  - Personal health data (≥ 10,000 U.S. persons)
  - Personal financial data (≥ 10,000 U.S. persons)
  - Biometric identifiers (>1,000 U.S. persons)
  - Human 'omic data (≥ 1,000 U.S. persons) or human genomic data (>100 U.S. persons)[8]
  - Precise geolocation data (≥ 1,000 U.S. devices)
- ✓ Commercial transactions with data that, when aggregated with other data, could exceed thresholds in a 12-month period
- ✓ Participation in data-sharing platforms, repositories, or consortia where clinical or research data may be contributed or received, and where foreign access or cumulative aggregation may occur over time
- ✓ Data shared with an entity outside the U.S. or with U.S.-based personnel who are covered persons
- ✓ Entities associated with:
  - China (including Hong Kong or Macau), Cuba, Iran, North Korea, Russia, or Venezuela, or
  - Any entity majority-owned or controlled by a party from one of the above countries

Other Guidance

The RPAC Guidance Memo on the Bulk Data Rule provides detailed instructions for assessing whether research contracts, data-sharing agreements, human 'omic data, and biospecimen transfers trigger restricted or prohibited transactions or may be exempt, and includes template contractual language campuses may use.

Campuses may also refer to NIH Notice NOT-OD-25-160, which establishes enhanced security and access control requirements for human biospecimens and associated data. While distinct from the DOJ Final Rule, these requirements may apply to overlapping datasets and should be considered as part of a coordinated research security and data governance approach.

For questions contact Christina Andersson (christina.andersson@ucop.edu) or Brian Russ (brian.russ@ucop.edu).

---

[3] *See*, DOJ Data Security Program: Compliance Guidance originally issued on April 11, 2025.
[4] eCFR :: 28 CFR 202.1101 -- Records and recordkeeping requirements.
[5] eCFR :: 28 CFR 202.1002 -- Audits for restricted transactions.
[6] eCFR :: 28 CFR 202.1001 -- Due diligence for restricted transactions.
[7] eCFR :: 28 CFR 202.248 -- Security requirements.
[8] See also NIH NOT-OD-25-160 for additional biospecimen security requirements

APPENDIX A: KEY DEFINITIONS[9]

Term	Definition
Access	Local or physical access, including the ability to obtain, read, copy, decrypt, edit, divert, release, affect, alter the state of, or otherwise view or receive, in any form, including through information systems, information technology systems, cloud-computing platforms, networks, security systems, equipment, or software. For purposes of determining whether a transaction is a covered data transaction, access is determined without regard for the application or effect of any security requirements.
Sensitive Personal Data	Data about U.S. persons of certain categories: covered personal identifiers, precise geolocation data, biometric identifiers, human `omic data, personal health data, personal financial data, or any combination thereof.
Bulk U.S. Sensitive Personal Data	A collection or set of sensitive personal data relating to U.S. persons, in any format, regardless of whether the data is anonymized, pseudonymized, de-identified, or encrypted, where such data meets or exceeds the applicable threshold set forth in § 202.205.
Government-Related Data	Any precise geolocation data, regardless of volume, for any location within any area enumerated on the Government-Related Location Data List in § 202.1401 which the Attorney General has determined poses a heightened risk of being exploited by a country of concern to reveal insights about locations controlled by the Federal Government, including insights about facilities, activities, or populations in those locations, to the detriment of national security, because of the nature of those locations or the personnel who work there. Such locations may include: (i) The worksite or duty station of Federal Government employees or contractors who occupy a national security position as that term is defined in 5 CFR 1400.102(a)(4); (ii) A military installation as that term is defined in 10 U.S.C. 2801(c)(4); or (iii) Facilities or locations that otherwise support the Federal Government's national security, defense, intelligence, law enforcement, or foreign policy missions. Any sensitive personal data, regardless of volume, that a transacting party markets as linked or linkable to current or recent former employees or contractors, or former senior officials, of the United States Government, including the military and Intelligence Community.
Country of Concern	Any foreign government that, as determined by the Attorney General with the concurrence of the Secretary of State and the Secretary of Commerce: (a) Has engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons; and

[9] eCFR :: 28 CFR Part 202 Subpart B -- Definitions

	(b) Poses a significant risk of exploiting government-related data or bulk U.S. sensitive personal data to the detriment of the national security of the United States or security and safety of U.S. persons.
U.S. Person	Any United States citizen, national, or lawful permanent resident; any individual admitted to the United States as a refugee under 8 U.S.C. 1157 or granted asylum under 8 U.S.C. 1158; any entity organized solely under the laws of the United States or any jurisdiction within the United States (including foreign branches); or any person in the United States.
Data Brokerage	The sale of data, licensing of access to data, or similar commercial transactions, excluding an employment agreement, investment agreement, or a vendor agreement, involving the transfer of data from any person (the provider) to any other person (the recipient), where the recipient did not collect or process the data directly from the individuals linked or linkable to the collected or processed data.
Investment Agreement	An agreement or arrangement in which any person, in exchange for payment or other consideration, obtains direct or indirect ownership interests in or rights in relation to: (1) Real estate located in the United States; or (2) A U.S. legal entity.
Employment Agreement	Any agreement or arrangement in which an individual, other than as an independent contractor, performs work or performs job functions directly for a person in exchange for payment or other consideration, including employment on a board or committee, executive-level arrangements or services, and employment services at an operational level.
Vendor Agreement	Any agreement or arrangement, other than an employment agreement, in which any person provides goods or services to another person, including cloud-computing services, in exchange for payment or other consideration.
Covered Data Transaction	Any transaction that meets **both** of the following: (1) involves **access** by a country of concern or a covered person to either government-related data or bulk U.S. sensitive personal data; and (2) is structured as a data brokerage, vendor agreement, employment agreement, or investment agreement.
Covered Person	(1) A foreign person that is an entity that is 50% or more owned, directly or indirectly, individually or in the aggregate, by one or more countries of concern or persons described in paragraph (a)(2) of this section; or that is organized or chartered under the laws of, or has its principal place of business in, a country of concern; (2) A foreign person that is an entity that is 50% or more owned, directly or indirectly, individually or in the aggregate, by one or more persons described in paragraphs (a)(1), (3), (4), or (5) of this section; (3) A foreign person that is an individual who is an employee or contractor of a country of concern or of an entity described in paragraphs (a)(1), (2), or (5) of this section;

	(4) A foreign person that is an individual who is primarily a resident in the territorial jurisdiction of a country of concern; or (5) Any person, wherever located, determined by the Attorney General: (i) To be, to have been, or to be likely to become owned or controlled by or subject to the jurisdiction or direction of a country of concern or covered person; (ii) To act, to have acted or purported to act, or to be likely to act for or on behalf of a country of concern or covered person; or (iii) To have knowingly caused or directed, or to be likely to knowingly cause or direct a violation of this part.

APPENDIX B: EXEMPTIONS[10]

Exempt Transaction	Description
Personal communications (§ 202.501)	This part does not apply to data transactions to the extent that they involve any postal, telegraphic, telephonic, or other personal communication that does not involve the transfer of anything of value.
Information or informational materials (§ 202.502)	This part does not apply to data transactions to the extent that they involve the importation from any country, or the exportation to any country, whether commercial or otherwise, regardless of format or medium of transmission, of any information or informational materials.
Travel (§ 202.503)	This part does not apply to data transactions to the extent that they are ordinarily incident to travel to or from any country, including importation of accompanied baggage for personal use; maintenance within any country, including payment of living expenses and acquisition of goods or services for personal use; and arrangement or facilitation of such travel, including nonscheduled air, sea, or land voyages.

[10] eCFR :: 28 CFR Part 202 Subpart E -- Exempt Transactions