FINAL

Response by the Centre for Information Policy Leadership to the DOJ's Proposed Rule on Preventing Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern

Docket No. NSD 104
Filed November 27, 2024

The Centre for Information Policy Leadership (CIPL)[1] welcomes the opportunity to respond to the Notice of Proposed Rulemaking published by the Department of Justice (DOJ) on October 29, 2024,[2] which proposes a rule to implement Executive Order 14117 of February 28, 2024 (Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern), by prohibiting and restricting certain data transactions with certain countries or persons.

CIPL thanks the DOJ for considering CIPL's response to the ANPRM [3] and, in particular, for providing thoughtful exemptions in the proposed rule. CIPL reiterates its appreciation for DOJ's commitment to advancing an approach consistent with "Data Free Flows with Trust." CIPL has published research on the importance of cross-border data flows for securing a wide range of economic and social benefits.[4] Any measures to address national security concerns associated with international transfers of Americans' personal data should be carefully designed to address those concerns without placing the broader benefits from data flows at risk.

We offer the following comments with a view to ensuring that certain aspects of the rule remove potential ambiguities and establish clear and appropriate guardrails for data transactions in countries of concern.

CIPL remains available to the DOJ should the agency desire further details or clarity on our suggestions.

---

[1] The Centre for Information Policy Leadership (CIPL) is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 85+ member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices to ensure the responsible and beneficial use of data in the modern information age. CIPL's work facilitates constructive engagement between business leaders, data governance and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at https://www.informationpolicycentre.com/. Nothing in this document should be construed as representing the views of any individual CIPL member company or of the law firm Hunton Andrews Kurth LLP. This document is not designed to be and should not be taken as legal advice.

[2] 89 FR 86116, available at https://www.federalregister.gov/documents/2024/10/29/2024-24582/provisions-pertaining-to-preventing-access-to-us-sensitive-personal-data-and-government-related-data.

[3] CIPL Response to U.S. Department of Justice Advance Notice of Proposed Rulemaking on Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern (April 1, 2024), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_doj_anprm.pdf.

[4] Please see CIPL, "The 'Real Life Harms' of Data Localization Policies, March 2023, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-tls_discussion_paper_paper_i_-_the_real_life_harms_of_data_localization_policies.pdf.

TABLE OF CONTENTS

Subpart B—Definitions

§ 202.206 – Bulk U.S. sensitive personal data.

The DOJ has chosen to define *bulk U.S. sensitive personal data* as a collection or set of bulk data relating to U.S. persons, in any format, regardless of whether the data is **anonymized**, **pseudonymized**, **de-identified**, or **encrypted**. However, the proposed rule does not define *anonymized*, *pseudonymized*, *de-identified,* or *encrypted*. These terms are used elsewhere in the rule, carrying great significance based on the context. See, for example, our discussion of *de-identified* versus *anonymized* in the context of exempt transactions under § 202.510, below. Given that these terms are not universally understood to mean the same thing in all contexts, it would be beneficial for the DOJ to clarify what they mean in the context of this proposed rule.

In addition to providing definitions for the terms mentioned above, we ask the DOJ to consider amending the definition of *bulk U.S. sensitive personal data* to provide an exemption for data encrypted with **post-quantum cryptography** (PQC). NIST has approved a suite of PQC algorithms

designed to withstand the attack of a quantum computer.[5] There is a need to drive adoption of these algorithms on a timeline relevant to the government's mandate to transition to these quantum-resistant algorithms by 2035. If the DOJ were to adopt a rule that incentivizes encryption via PQC algorithms, this effort would be an important opportunity to make progress toward the goal on PQC adoption. This would also help to build a case to exempt PQC encrypted data.

§ 202.211 – Covered Person

The preamble to the NPRM states that "[t]he proposed rule would not treat any U.S. person, including a U.S. subsidiary of a covered person, as a covered person unless the Department has designated the U.S. subsidiary as a covered person pursuant to the process described in the proposed rule. No U.S. person, including the U.S. subsidiary of a covered person, would be categorically treated as a covered person under the proposed rule."[6]

While it is helpful that U.S. subsidiaries of covered persons are not categorically *covered persons* under the rule, § 202.211(a)(5), read together with §202.701, grants the Attorney General extraordinarily broad authority to designate as covered persons those persons or entities who are not already covered by the proposed rule. This includes persons or entities who DOJ believes are "*likely* to become owned or controlled by or subject to the jurisdiction or direction of a country of concern or covered person"; "*likely* to act for or on behalf of a country of concern or covered person"; or "*likely* to knowingly cause or direct a violation of this part."[7] As drafted, the proposed rule appears to authorize the DOJ to designate a person or entity as a *covered person* based entirely on speculative or theoretical risks. It is possible that some U.S. companies could restrict data transfers to other U.S. (or foreign) parties based on concerns that those parties could be designated by DOJ in the future as *covered persons*.

The broad designation powers set forth in § 202.211(a)(5) and §202.701 should provide more guidance for entities (and specifically U.S. subsidiaries) that endeavor to take substantive and meaningful steps to avoid designation. For example, U.S. subsidiaries of covered entities that take steps to implement the CISA requirements described in the NPRM could still be at risk of designation. At a minimum, DOJ should clarify that implementation of the CISA requirements by U.S. subsidiaries of covered companies would affirmatively factor against designation.

§ 202.214 – Data brokerage.

While CIPL recognizes that the DOJ has chosen not to amend the definition of *data brokerage* to include a blanket exception for service providers and others data processors operating pursuant to a data processing agreement,[8] CIPL asks the DOJ to recognize that where a processor is not buying, leasing, or otherwise acquiring rights in the data (i.e., not engaged in a "similar commercial

---

5 *NIST Releases First 3 Finalized Post-Quantum Encryption Standards* (August 13, 2024), available at https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards.

6 89 FR at 86150, available at https://www.federalregister.gov/d/2024-24582/page-86150.

7 § 202.211(a)(5)(i)-(iii) (emphasis added).

8 89 FR at 86130-31, available at https://www.federalregister.gov/d/2024-24582/page-86130.

transaction"), the NPRM's provisions relating to **vendor agreements**, rather than data brokerage, would apply.

§ 202.241 – Personal heath data.

Section 202.241 defines "personal health data" as health information that **"relates to"** the past, present, or future physical or mental health or condition of an individual. CIPL asks the definition to be limited to information that **"reveals"** (rather than "relates to") a particular individual's physical or mental health condition. Information that is *related to* but does not *reveal* the individual's health condition could unnecessarily restrict commerce and access to useful goods and services (e.g., fitness products or programs) without a corresponding reduction in potential harm.

§ 202.249 – Sensitive personal data.

The definition of *sensitive personal data* does not clearly distinguish between the data of individuals as users or consumers (on the one hand) and the data of individuals or businesses acting in the capacity of a business (on the other hand). While it is quite clear that the former category is in scope, it is not clear whether the latter category is in scope. CIPL asks the DOJ to clarify.

Subpart C—Prohibited Transactions and Related Activities

§ 202.302 – Other prohibited data-brokerage transactions involving potential onward transfer to countries of concern or covered persons.

Section 202.303 includes a prohibition specific to data brokerage to address transactions involving the onward transfer or resale of government-related data or bulk U.S. sensitive personal data to countries of concern and covered persons. With respect to the need for **contractual restrictions** in data brokerage transactions with foreign persons, we ask the DOJ to clarify that the regulation does not apply to agreements entered into *prior to the effective date*. If, however, the DOJ determines that the regulation applies to agreements entered into prior to the effective date, we request that the DOJ provide sufficient time for U.S. companies *to amend existing agreements*.

§ 202.304 – Prohibited evasions, attempts, causing violations, and conspiracies.

The NPRM includes examples intended to highlight how the NPRM would "apply in certain scenarios where bulk U.S. sensitive personal data would be licensed or sold to support algorithmic development … or where sensitive personal data could be extracted from artificial intelligence models."[9] We suggest that DOJ substantially refine, or consider omitting, the examples provided. Some AI models are not trained using personal data, and in instances where they are, there is an active debate about the extent to which algorithms should be understood to "contain" personal data, as characterized in Example 6 in § 202.304(b).[10]

---

[9] 89 FR at 86132, available at https://www.federalregister.gov/d/2024-24582/page-86132. Relatedly, see § 202.304(b) Ex.6; § 202.214 Ex. 6; § 202.217 Ex. 4; and § 202.301 Ex. 1.

[10] For example, please see https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/-Datenschutz/Informationen/240715_Discussion_Paper_Hamburg_DPA_KI_Models.pdf.

Given that the mitigation of risks surrounding the disclosure of sensitive data by AI models/systems is an area of active study and emerging best practices, the DOJ should proceed carefully with guidance for such scenarios. One possibility would be for the DOJ to consider adopting an "actual knowledge" standard as it relates to risks that particular models could be inappropriately prompted ("jail-broken") to divulge sensitive data.

Subpart E—Exempt Transactions

§ 202.505 – Financial services

CIPL welcomes the banking and payment services exemption, but given the complexity of this area, we seek further clarification on the scope of the exemption.

1. **§ 202.505(b) - Example 10.** We recommend amending Example 10 to provide clarification that a **"lawful request"** is based on the **laws of the country of concern**. We seek confirmation that responding to a request that is (1) lawful under the laws of the country of concern, (2) from a regulator of a country of concern, and (3) in reference to financial activities within the scope of the Financial Services Exemption, should be considered "ordinarily incident to the provision of financial services" and should therefore be exempt. Compliance with such requests is part of doing business in the country of concern, as such requests are for a lawful purpose under the laws of the country of concern. Further, not being able to respond to such requests would put companies in a conflict-of-laws position. We therefore recommend the following changes to Example 10:

   Example 10. *A U.S. ~~bank~~ financial services provider operates a foreign branch, subsidiary, or affiliate in a country of concern and provides financial services to U.S. persons living within or visiting the country of concern. The ~~bank~~ financial services provider, its foreign branch, subsidiary, or affiliate receives a ~~lawful~~ request that is lawful under the laws of the country of concern from ~~the~~ a regulator or law enforcement authority in the country of concern to review the financial activity conducted in the country, which includes providing access to the bulk sensitive personal data of U.S. persons resident in the country or U.S. persons conducting transactions through the foreign branch, subsidiary, or affiliate. Responding to the ~~regulator's~~ request of the regulator or law enforcement authority, including providing access to this bulk sensitive personal data, is ordinarily incident to the provision of financial services and is exempt.*

2. **§ 202.505(b) – New Example.** We suggest an **additional example** complementary to Example 11 to clarify that data transfers may be required both *reactively* in relation to a government request as well as part of *routine* reporting requirements, such as quarterly reports or ad hoc information requests for China inbound transactions (U.S. persons or cardholders transacting at a China merchant) to regulators or law enforcement authorities in China, e.g., the State Administration of Foreign Exchange or the People's Bank of China (PBOC, the Central Bank). These are reports or information requests required under the laws, regulations, or guidance pursuant to the laws of the country of concern. We have suggested a new example to cover this activity:

   New Example: *A U.S. financial services provider operates a foreign branch, subsidiary, or affiliate in a country of concern and provides financial services to U.S. persons living within or visiting the country of concern. The financial services provider, its foreign branch, subsidiary, or affiliate is subject to reporting requirements imposed by a regulator or law enforcement authority with jurisdiction over it in the country of concern. Compliance with the reporting requirements includes providing access to*

the bulk sensitive personal data of U.S. persons resident in the country or U.S. persons conducting transactions through the foreign branch, subsidiary, or affiliate. Compliance with the regulator's reporting requirements, including providing access to this bulk sensitive personal data, is ordinarily incident to the provision of financial services and is exempt.

3. **§ 202.505(b) – Second New Example.** We suggest an additional example to make it clear that **cybersecurity services** may be considered ancillary to processing payments and funds transfers, for example, as being a form of risk mitigation and prevention.

   ***New Example**: A U.S. company that provides payment-processing services for cross-border payment transactions sells cybersecurity services to financial institutions, merchants, and other payment recipients that are incorporated in, located in, or subject to the jurisdiction of a country of concern. The services are ancillary to the payment processing and are designed to prevent or identify potentially fraudulent or otherwise nefarious cross-border payments to such parties. To provide the services, the U.S. company engages in data transactions to transfer bulk U.S. sensitive personal data such as IP addresses, email addresses, and device information, along with financial data, to such parties. Both the U.S. company's transaction transferring bulk U.S. sensitive personal data and the payment transactions by U.S. individuals are exempt transactions.*

4. **§ 202.505(b) – Third New Example.** We suggest a third new example to address **product development** issues. While Example 4 of § 202.506 clarifies that sending bulk personal financial data for the purposes of developing a financial software tool is *not* ordinarily incident to and part of *administrative or ancillary business operations*, product development may be "ordinarily incident to and part of the *provision of financial services*" under § 202.505, particularly in the development of fraud and cybersecurity services in the global payment ecosystem. Fraud trends that appear in one region or country will quickly appear in others. Thus, to build effective fraud detection and prevention models and to gain the necessary insights into fraudulent activity in order to prevent them, these models must be built using global or multi-country data sets. Further, as data needs to be analyzed together as a whole to spot patterns of fraud, leaving out certain data from the analysis will deprive the models of the training required to accurately detect fraud. We recommend the inclusion of a new example as follows.

   ***New Example**: A U.S. financial services provider transfers U.S. bulk sensitive data to a foreign branch, subsidiary, or affiliate located in a country of concern as ordinarily incident to and part of the process of developing or improving its financial products and services related to cybersecurity and combating fraud. The transfer is exempt.*

§ 202.506 – Corporate group transactions.

CIPL supports the proposed exemption for "corporate group transactions," and we appreciate that the proposed exemption includes examples of activities that fall within the exemption, such as employees' internal and external communications. However, we believe that multinational companies are put at a significant disadvantage given the limitations of the intra-entity transaction exemption because, as currently drafted, the intra-entity exemption could exclude other ordinary workplace activities and business operations. We suggest that the list of examples under § 202.506(a)(2) also include the following **routine, low-risk transactions**:

- Internal collaboration and review platforms;
- Pricing and billing systems;

- Customer and vendor relationship management tools, **including technical assistance centers;**
- Expense monitoring and reporting;
- Recruiting and activities related to identifying, referring, assessing, communicating with, and selecting job applicants or potential job applicants;
- Contingent workforce management; and
- Financial planning, analysis, and management activities.

We also believe that the exemption should be expanded to include the **tools** that support corporate transactions, for example, recruitment and human resource management platforms; internal and external communication and document management resources; email and video conferencing platforms; enterprise application software; customer and vendor relationship management and onboarding; expenses and travel booking platforms, etc.

In addition, we note that the exemption has been formulated to indicate that it may only be used to exempt ancillary business operations to the extent they are *ordinarily incident to and part of administrative or ancillary internal business operations*. The exemption should also cover operations that are **required for global operations of a service related to U.S. persons**. We suggest adding the following example to clarify this point:

> ***§ 202.506(b)- New Example:*** *A U.S. company that is a financial services provider has a foreign subsidiary located in a country of concern. Customers of the U.S. company conduct financial transactions in the country of concern, and customers of the foreign subsidiary conduct transactions in the U.S. The foreign subsidiary accesses bulk U.S. sensitive personal data, more particularly personal financial data, from the U.S. company to perform customer service functions related to these transactions. This is an exempt corporate group transaction.*

§ 202.509 – Telecommunications services.

The proposed rule exempts transactions that are ordinarily incident to and part of telecommunications services. While we support the inclusion of an exemption for telecommunications services, it may be too narrow to adequately address the broader scope of networking, IT infrastructure, and related services. Telecommunications is just one component of a much larger ecosystem of interconnected services, so CIPL recommends expanding the exemption to say "**telecommunications, networking, and related services**."

§ 202.510 – Drug, biological product, and medical device authorizations.

Under the proposed rule, certain data transactions necessary to obtain and maintain regulatory approval to market a drug, biological product, medical device, or combination product in a country of concern would be exempt from the prohibitions in the proposed rule. This exemption, however, is limited to data that is **de-identified.**

Significantly, the term *de-identified* is not defined in the proposed rule.

Pharmaceutical companies and others seeking to obtain and maintain regulatory approval need clarity on what *de-identified* means in this context. Some companies are accustomed to applying HIPAA's

standard for de-identification (45 CFR § 164.514(a) and (b)), but it is unclear whether that standard would apply here.[11]

The preamble to the proposed rule appears to suggest that the de-identification that takes place for post-market pharmacovigilance reporting to FDA would be the applicable standard.[12] **CIPL asks the DOJ to confirm that it intends to adopt the FDA's *post-marketing safety reporting deidentification standard* in this context.** Additionally, the DOJ may include a reference to another industry standard familiar to companies in the pharmaceutical industry, namely the International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use Good Clinical Practice (ICH GCP), which includes the definition of "subject identification code"[13]

Moreover, Example 2 under § 202.510(d)(2) uses the term *de-anonymized* in the context of data losing its "de-identified" status, raising the question of whether ***anonymized*** and ***de-identified*** are to be viewed as **synonymous**. Definitions of *de-identified* and *anonymized* could help clarify whether that is the case and, if so, whether uses of the term *anonymized* in other parts of the proposed rule, such § 202.206, are superfluous.

The rule should also clarify whether "**key-coded data**" may constitute "regulatory approval data" within the scope of § 202.510's exemption. Pharmaceutical companies commonly use key-coded data for research purposes, and such data is required to support the regulatory approval process and post-marketing approval requirements. Guidance published by the Food and Drug Administration (FDA-2008-D-0199 [14]) recognizes the use of **single-coded data** as the current standard for clinical research because, as explained in the guidance, the use of such data allows for clinical monitoring, subject follow-up, or the addition of new data from the subject.[15] The guidance also mentions the use of **double-coded data** to provide "additional confidentiality and privacy protection for subjects."[16] The guidance notes, however, that both single- and double-coded data may be traceable to a given individual with the use of the coding key(s). That said, **if key-coded data were *not* to fall within the**

---

[11] It should be noted that the HIPAA standard may not be appropriate in the clinical trial context, as it would require the removal of all dates, including enrollment and treatment dates.

[12] *Id.*, at 86139, available at https://www.federalregister.gov/d/2024-24582/page-86139. 21 C.F.R. § 314.80(i) provides: "An applicant should not include in reports under this section the names and addresses of individual patients; instead, the applicant should assign a unique code for identification of the patient. The applicant should include the name of the reporter from whom the information was received as part of the initial reporter information, even when the reporter is the patient."

[13] *See* **1.58. Subject identification code**: "A unique identifier assigned by the investigator to each trial subject to protect the subject's identity and used in lieu of the subject's name when the investigator reports adverse events and/or other trial related data." *See also* **5.5. Trial management, data handling, and record keeping:** "5.5.5. The sponsor should use an unambiguous subject identification code (see 1.58) that allows identification of all the data reported for each subject." Available at https://www.ema.europa.eu/en/ich-e6-r2-good-clinical-practice-scientific-guideline.

[14] *Guidance for Industry: E15 Definitions for Genomic Biomarkers, Pharmacogenomics, Pharmacogenetics, Genomic Data and Sample Coding Categories*, published April 2008 by the FDA's Center for Drug Evaluation and Research (CDER) and Center for Biologics Evaluation and Research (CBER), available at https://www.fda.gov/regulatory-information/search-fda-guidance-documents/e15-pharmacogenomics-definitions-and-sample-coding.

[15] *Id.*, p.5.

[16] *Id.*

scope of the exemption, the exemption itself would not achieve its intended effect, since key-coded data is required to support the regulatory approval process.

Given the confusion generated by use of *de-identified* in this context, CIPL asks the DOJ to permit the use of ***pseudonymized*** data (in addition to de-identified data) for purposes of this exemption, and to define *pseudonymized* so as to cover key-coded data.

Moreover, to eliminate any potential confusion when data is required to be submitted to more than one ***regulatory entity*** in a country of concern, CIPL suggests that the use of the term in § 202.510(b) be amended to encompass the plural—***regulatory entity(ies)***—as several entities, both at national and local levels, can be involved in authorizing clinical research and/or reviewing safety and efficacy data necessary to obtain or maintain regulatory approval of covered products.

Example 3 under § 202.510(d)(3) **prohibits the use of vendors** to store, organize, and prepare bulk U.S. sensitive personal data for submission to the regulatory agency in a country of concern. While the preamble to § 202.510 notes that "[e]mployment and vendor transactions in this context would be *restricted*, not *prohibited*, transactions, and generally could proceed if the requirements applicable to restricted transactions were followed,"[17] that distinction is not clear from the text of the proposed rule and should be made explicit.

That said, inasmuch as the data at issue is **ultimately being shared with the regulatory agency** in the country of concern, there appears to be little rationale for applying the burdensome requirements for restricted vendor transactions in this context.

For many pharmaceutical companies, the use of vendors is required as part of a clinical trial or pharmacovigilance program or as a local distributor in a country of concern. Given the specialized nature of the industry, pharmaceutical companies must rely on highly qualified, knowledgeable vendors on the ground in locations across the globe. Some countries, including China, require a local agent when submitting a clinical trial or marketing application to regulators for approval. The local agent is supposed to be the liaison to the local regulator, hold the online account for submission, and be the source of answers to technical questions in the local language. If a pharmaceutical company cannot use a local affiliate or a local distributor for the submission, then the company is effectively banned from submitting the data for drug approval.

Given that many countries, including China, mandate that only locally incorporated entities can submit regulatory filings, the exemption as written undermines its intended purpose. It creates significant barriers for U.S. companies to deliver innovative treatments to patients in these regions, contradicting the DOJ's stated goal of avoiding disruption to commercial and scientific relationships.

To address this inconsistency, we suggest proposing the deletion of Example 3 from Section 202.510(d)(3) and explicitly clarifying that the exemption applies to all data transfers necessary for regulatory approvals, including transfers to local entities when required by local law. It should also clarify that the general prohibition on data transactions that involve bulk human genomic data (see § 202.303), would not apply to the use of vendors in this context. These adjustments would ensure that the exemption achieves its intended purpose of supporting U.S. biopharmaceutical innovation while maintaining national security.

---

[17] 89 FR 86116, at 86138 (emphasis added), available at https://www.federalregister.gov/d/2024-24582/page-86138.

Thus, in response to the DOJ's question,[18] vendor agreements should be considered to be "ordinarily incident to and part of" a clinical trial or marketing application.

As for **employment** transactions, the rule should clarify that company employees in a country of concern are likewise allowed to support these exempt processes for the same reasons.

§ 202.511 – Other clinical investigations and post-marketing surveillance data.

The proposed rule provides exemptions for clinical research in countries of concern, but the preamble notes that the DOJ "is considering whether any exemption, or parts of it, could feasibly be **time-limited** to allow industry to shift existing processes and operations out of countries of concern over a transition period."[19] While the quoted language appears in the preamble relating to § 202.511, CIPL reads it as applying equally to § 202.510, and therefore our comments below pertain to both provisions.

CIPL submits that the potential phase-out of the exemptions could cause significant harm. In particular, the inability to use data to support market authorizations would:

- significantly increase the cost and duration of drug development by necessitating additional clinical trials to make up for the loss of patients required to show statistical significance;
- disrupt global clinical trials, threaten scientific progress, and reduce the diversity and scalability of clinical trials (as diverse populations have significant biological differences that translate into better data and more personalized, effective, and safer medicines);
- disrupt the global clinical trial cooperation framework;
- withhold the availability of beneficial drugs from a large number of potential beneficiaries—including U.S. patients—raising ethical concerns;
- prevent U.S. companies from marketing new drugs in countries of concern and ultimately force them to cease operations in these regions altogether (in the long term);
- hinder revenue generation for U.S. companies, weakening their ability to reinvest in research and development, while shifting the financial burden to U.S. patients, who would face potentially higher health care and drug costs as R&D costs rise; and
- cause U.S. companies to lose their competitive edge, as foreign competitors fill the void in these markets.[20]

---

[18] "The Department seeks comments on whether such a vendor agreement should be considered to be 'ordinarily incident to and part of' a clinical investigation; how prevalent and important the practice of sending bulk U.S. sensitive personal data to a covered person in a country of concern is; and the potential impacts to clinical research, medical product development and authorization, and industry if such transactions were restricted or prohibited." 89 FR at 86139, available at https://www.federalregister.gov/d/2024-24582/page-86139.

[19] 89 FR at 86140, available at https://www.federalregister.gov/d/2024-24582/page-86140.

[20] "As of 2019, China was the world's second-largest pharmaceutical market, following the United States with a market share of around 8.5 percent in global pharmaceutical sales." *Retail trade revenue of traditional Chinese and western medicine in China December 2011 to December 2023*, Statista, available at https://www.statista.com/statistics/226906/trade-revenue-of-medicine-in-china-by-month/.

Subpart H – Licences; Subpart J - Due Diligence and Audit Requirements; Subpart K - Reporting and Recordkeeping Requirements; Subpart L - (Submitting Applications, Requests, Reports; and Subpart M - (Penalties and Finding of Violation)

The administrative and organizational requirements covered Subparts H, J, K, L, and M are reflected, at a high level, in privacy programs and privacy frameworks already in use by many organizations. Where possible and appropriate, DOJ should enable voluntary certification programs that organizations may use to demonstrate compliance with the requirements of this rule.