Westlaw Today

Proposed rule on protecting bulk sensitive data and its impact on health care

By Jodi G. Daniel, Esq., Linda Malek, Esq., Jason Johnson, Esq., and Evan Y. Chuck, Esq., Crowell & Moring LLP*

DECEMBER 6, 2024

On October 29, 2024, the Department of Justice (DOJ) published a Notice of Proposed Rulemaking (NPRM, https://bit.ly/4i6HemQ) to implement Executive Order 14117 (https://bit.ly/3ZaeiBX) "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern" (the E.O.).

The E.O. addresses the national security threat posed by the continued effort of certain countries of concern to access and exploit certain kinds of Americans' sensitive personal data, which includes health data and genetic data. This builds on DOJ's Advance Notice of Proposed Rulemaking (ANPRM) published on March 5. Comments were due on November 29, 2024.

Overview

This NPRM proposed to establish rules for certain data transactions that pose an unacceptable risk of giving "countries of concern" or "covered persons" access to government-related data or bulk U.S. sensitive personal data (Affected American Data).

Among other things, the NPRM identifies classes of prohibited and restricted transactions, identifies countries of concern and classes of covered persons to whom the proposed rule applies, identifies classes of exempt transactions, explains DOJ's methodology for establishing bulk thresholds, and establishes processes to issue licenses authorizing certain prohibited or restricted transactions.

- *Countries of concern*: China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia, and Venezuela.
- *Covered persons*: (1) foreign entities that are 50 percent or more owned by a country of concern, organized under the laws of a country of concern, or has its principal place of business in a country of concern; (2) foreign entities that are 50 percent or more owned by a covered person; (3) foreign employees or contractors of countries of concern or entities that are covered persons; and (4) foreign individuals primarily resident in countries of concern.
- *Sensitive personal data*: There are 6 categories of "sensitive personal data," including personal health data, biometric data, and human genomic data.
- *Bulk sensitive personal data*: The NPRM proposes thresholds for "bulk" sensitive data based on a risk-based analysis, considering the threats, vulnerabilities, and consequences associated with the human-centric and machine-centric characteristics of each type of data.

The proposed rule does not proport to restrict data flow more generally or require data localization. Rather, the proposed rule is meant to limit data transfers in very specific circumstances. Therefore, it is important to understand what data exchanges the DOJ is attempting to prohibit or restrict.

DOJ is concerned that large human genetic datasets that are used for ancestry, solving crimes, and research can be misused for counterintelligence purposes.

For transactions that are restricted, the proposed rule imposes security requirements on specific kinds of commercial transactions — vendor agreements, employment agreements, and investment agreements.

Specifically, these commercial transactions would need to comply with the separately proposed organizational and system-level security requirements and data-level requirements that have been developed by the Department of Homeland Security's Cybersecurity and Infrastructure Agency (CISA). CISA is concurrently making these proposed security requirements (https://bit.ly/3CKNfFz) available for public comment.

The proposed rule also impacts data brokerage transactions related to sensitive bulk data, including health and genomic data (which includes de-identified data).

Data brokerage transactions are defined broadly as the "sale of data, licensing of access to data, or similar commercial transactions

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."

Impact on health data

The NPRM focuses on six different types of sensitive data, including personal health and human genomic data, and the risks involved with each. It relies on HIPAA in part to define "personal health data" but the definition varies in significant ways.

First, the definition of "personal health data" in the NPRM includes de-identified data that would not be subject to HIPAA, a point that is highlighted in the preamble. DOJ explains that de-identified, pseudonymized or anonymized data could reveal exploitable, sensitive information.

Second, the definition includes specific examples of data that would be "personal health data," including basic physical measurements and health attributes; social, psychological, behavioral, and medical diagnostic, intervention, and treatment history; test results; logs of exercise habits; immunization data; data on reproductive and sexual health; and data on the use or purchase of prescribed medications.

In describing the risk to health data, DOJ seems to criticize the market for health care data, calling out hospitals, medical facilities, pharmaceutical companies, insurers, and pharmacies.

DOJ notes that there is "a large market for such data, which generates significant profits for companies with the capabilities to collect, anonymize, collate, and sell the data to third parties and data brokers," that "the keepers of this data will take advantage of the increasing demand and massive economic benefits that these data sales can achieve," and that "data brokers have flourished by selling packaged datasets on the sensitive health conditions of millions of Americans in the open market."

The definition of "data brokerage" is so broad that it would also seem to include the licensing of data from data repositories or bio repositories, the creation of which have become more commonplace in recent years as academic medical centers and other companies have used these repositories for data monetization.

Given that the DOJ declined to exclude information that is de-identified, pseudonymized or aggregated from the proposed rule's scope (other than the clinical trial collection exemption listed below), this could have implications for the sharing and exchange of information for certain research purposes.

For example, it is unclear in the rare disease area if and when the removal of certain amounts or types of information, such as demographic information, would qualify a transaction for exemption from the proposed rule.

The NPRM also includes discussion about the high concern and sensitivity regarding human genetic and genomic data (as compared with moderate sensitivity of health and claims data). DOJ notes that human genomic data that is important to design a disease therapy can also be used "to identify genetic variability in a population, which can potentially be used for nefarious purposes such as identifying and exploiting susceptibility to disease."

DOJ is concerned that large human genetic datasets that are used for ancestry, solving crimes, and research can be misused for counterintelligence purposes. The DOJ is considering expanding regulated transactions to include certain other 'omic data, such as epigenomic data and transcriptomic data, and has asked for public feedback on potential benefits and risks to include involving these other 'omic categories, which means that the scope of this proposed rule may further expand to include other types of data and information.

In discussing the sensitivity of these types of data, DOJ identifies particular examples and concerns related to health care, including that China and Chinese companies "have sought to acquire sensitive health and genomic data on U.S. persons through, for example, investment in U.S. firms that handle such data or by partnering with healthcare or research organizations in the United States to provide genomic sequencing services."

The NPRM would establish bulk thresholds based on sensitivity. For human genomic data, "bulk data" would include data on over 100 U.S. persons. For personal health data, "bulk data" would include data on over 10,000 U.S. persons. However, if personal health data is combined with other data types with lower thresholds, it would need to meet the lowest threshold for any category in the dataset.

Another potential impact on health care entities is the obligation for U.S. entities involved in data brokerage related transactions to perform due diligence on non-U.S. entities before exchanging any data and entering into contracts that require a prohibition on the entity receiving the data from using the data for any additional transactions that would be a covered transaction under the proposed rule.

The DOJ expects that any U.S. entity that is involved in such a data brokerage transaction would "take reasonable steps to evaluate whether their foreign counterparties are complying with the contractual provision as part of implementing risk-based compliance programs under the proposed rule." Failure to do so could subject health care entities to enforcement actions.

Exemptions

The NPRM would exempt certain classes of data transactions, a couple of which focus on health care.

Specifically, the following data transactions would be exempt:

- *Transactions necessary for drug, biological product, and medical device authorizations* would be exempt if the data transactions involve "regulatory approval data" necessary to obtain or maintain regulatory approval in a country of concern. "Regulatory approval data" would mean de-identified sensitive personal data required by a regulatory entity to research or market a drug, biological product, device, or combination product, including post-marketing studies and surveillance, but excludes data not necessary for assessing safety and

effectiveness. The DOJ notes, however, that this exemption does not cover all uses of the information related to regulatory approval, explicitly refusing to expand the exemption to cover vendor or employment agreements to prepare data for submission, making it important to consider the actual data use in determining if this exemption applies.

- *Grants, contracts or other agreement entered into with the United States Government*, most notably exempting grantees and contactors of the Department of Health and Human Services (which include the National Institutes of Health) and National Science Foundation from the proposed rule.
- *Transactions that are part of other clinical investigations and post-marketing surveillance* if the transactions:
    - are part of clinical investigations regulated by the Food and Drug Administration (FDA) under sections 505(i) or 520(g) of the Federal Food, Drug, and Cosmetic Act;
    - support FDA applications for research or marketing permits for drugs, biologics, devices, combination products, or infant formula; or
    - are part of the collection or processing of clinical care data indicating real-world performance or safety of products, or post-marketing surveillance data necessary to support or maintain FDA authorization, provided the data are de-identified.

Sharing data with Chinese parties: China Anti-Foreign Sanctions Law (AFSL) implications

If data is being shared with Chinese parties (such as in drug or medical device development), it will be important to understand how the final rules may impact new or existing business relationships with Chinese parties — particularly how compliance with the final rules will be communicated to those Chinese parties. If business relationships must be suspended or terminated, such action could violate Chinese law.

China is ramping up enforcement of its Anti-Foreign Sanctions Law, which can trigger Chinese investigations and retaliatory government action if compliance with U.S. law is deemed to be "discriminatory" against Chinese contract parties. Compliance with the final rules could be deemed to be "discriminatory" by Chinese parties.

China recently initiated an investigation of the parent company of Calvin Klein and Tommy Hilfiger for its efforts to comply with the U.S. Uyghur Forced Labor Prevention Act. In addition, the AFSL provides aggrieved Chinese parties with the right to sue multinational companies for alleged discriminatory activities (such as failure to execute a transaction or to terminate an existing agreement) that could arise if multinational companies comply with the final rules.

Conclusion

This rule, if finalized, may have a significant impact on partnerships, research, uses of data, and other activities where health care organizations are working with entities in countries of concern. It may also suggest concerns by the federal government about data security and data sharing more broadly and could reflect broader considerations on health data protections in other regulations.

We encourage health care organizations to review this rule and consider commenting. The NPRM specifically invites comments on the scope of the exemptions for transactions related to drug and medical device authorizations and clinical investigations and surveillance. There was only a 30-day comment period, which ended on November 29. (Note: the due date was the day after Thanksgiving). The timing suggests that DOJ may be trying to finalize this before the change in Administration on January 20, 2025.

Please note the request by the DOJ that comments include specific information that can help them incorporate feedback easier, specifically: (1) submit a short executive summary at the beginning of all comments; (2) provide supporting material, including empirical data, findings, and analysis in reports or studies by established organizations or research institutions; (3) describe the relative benefits and costs of the approach contemplated in this NPRM and any alternative approaches; and (4) refer to the specific proposed subpart or defined term to which each comment is addressed.

About the authors




(L-R) **Jodi G. Daniel** is a partner at **Crowell & Moring LLP** and a managing director at its strategic consulting firm, Crowell Health Solutions, in Washington, D.C. She was a founding director at the Office of the National Coordinator for Health IT at the U.S. Department of Health and Human Services. Daniel counsels technology companies, health care providers, health plans and life science companies on regulatory and policy issues related to digital health, including data access and use, privacy and security, interoperability, health information exchange, information blocking, telehealth, FDA oversight, and artificial intelligence. Daniel can be reached at jdaniel@crowell.com. **Linda Malek** is a partner in the firm's health care and privacy and cybersecurity groups in New York, and a managing director at Crowell Health Solutions. She advises a broad array of health care and life sciences clients on compliance with federal, state and international law governing clinical research, data privacy, cybersecurity, and fraud and abuse. Malek can be reached at lmalek@crowell.com. **Jason Johnson**, also a partner in the firm's health care and privacy and cybersecurity groups in New York, draws on his experience as a former research scientist to advise clients on complex compliance, legal, regulatory and transactional matters. He helps clients in the health care and life sciences industries navigate data privacy and cybersecurity issues under U.S. and European law and offers strategic insights on product development, marketing, clinical research and other core business initiatives. Johnson can be reached at jjohnson@crowell.com. **Evan Y. Chuck** is a partner in the firm's international trade group in Los Angeles and head of its Asia practice. Using his 30 years of corporate and international trade experience representing companies and private equity firms in their cross-border investments, he acts as a strategic adviser to corporate executives and helps with creating and executing risk mitigation strategies, particularly those that involve "de-risking" China business exposure. Chuck can be reached at echuck@crowell.com. The authors would like to thank senior counsel Stephen Holland for contributing to this article, which was originally published Nov. 6, 2024, on the firm's website. Republished with permission.

This article was published on Westlaw Today on December 6, 2024.