PUBLICATION

DOJ Bulk Data Rule: Key Takeaways for Healthcare and Life Sciences

Authors: Michael J. Halaiko, Alexandra P. Moylan, Julie A. Kilgore
May 21, 2025

The Data Security Program (DSP), implemented by the Department of Justice's National Security Division (DOJ/NSD) under Executive Order 14117 (Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern), became effective on April 8, 2025. The DOJ/NSD issued additional guidance on April 11, 2025, to assist U.S. organizations in understanding and complying with the DSP.

In our prior alert, we provided an overview of the guidance documents. In this alert, we focus on what U.S. health care and life science organizations need to know about compliance with the DSP. Focusing on internal policies and processes needed for compliance now, before the limited enforcement period ends on July 8, 2025, is critical for such organizations, given the type of sensitive data they collect, maintain, and process.

Does the DPS Cover Data Typically Processed by U.S. Health Care and Life Science Organizations?
Yes. U.S.-based health care and life science organizations are undoubtedly processing sensitive personal data as part of their core functions. There are six categories of sensitive data regulated by the DSP which are broadly defined. Unlike most other national and international privacy laws and regulations, anonymization, pseudonymization, de-identification or encryption does not alone exempt the data from the DSP, a subject covered in one of our prior alerts.

Of the six categories of sensitive personal data regulated under the DSP, several are routinely processed by health care and life science organizations including: (1) human 'omic data; (2) biometric data; and (3) personal health information. Human 'omic data includes "genomic data," "epigenomic data", "proteomic data," and "transcriptomic data" as defined in Table 1. Biometric data includes "measurable physical characteristics or behaviors," such as facial images, voice prints, and fingerprints. Personal health data is likely the most common form of sensitive data processed by health care and life science organizations and includes medical records, test results, and immunization data.

Category of Data	Definition
Human genomic data	Data representing the nucleic acid sequences that constitute the entire *set* or a subset of the genetic instructions found in a human cell, including the result or results of an individual's 'genetic test' (as defined in 42 U.S.C. 300gg–91(d)(17)) and any related human genetic sequencing data.
Human epigenomic data	Data derived from a systems-level analysis of human epigenetic modifications, which are changes in gene expression that do not involve alterations to the DNA sequence itself. These epigenetic modifications include DNA methylation, histone modifications, and non-coding RNA regulation. Routine clinical measurements of epigenetic modifications for individualized patient care purposes would not be considered epigenomic

	data under this rule because such measurements would not entail a systems-level analysis of the epigenetic modifications in a sample.
Human proteomic data	Data derived from a systems-level analysis of proteins expressed by a human genome, cell, tissue, or organism. Routine clinical measurements of proteins for individualized patient care purposes would not be considered proteomic data under this rule because such measurements would not entail a systems-level analysis of the proteins found in such a sample.
Human transcriptomic data	Human transcriptomic data. Data derived from a systems-level analysis of RNA transcripts produced by the human genome under specific conditions or in a specific cell type. Routine clinical measurements of RNA transcripts for individualized patient care purposes would not be considered transcriptomic data under this rule because such measurements would not entail a systems-level analysis of the RNA transcripts in a sample.

Table 1

Critically, personal health data is not limited to data collected only by medical and health care professionals and institutions – DOJ's guidance confirms that "personal health data" is not limited to Protected Health Information or data collected by covered entities as regulated by HIPAA. It is data collected or held by *any entity* that indicates, reveals, or describes the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual. It includes basic physical measurements and health attributes (such as bodily functions, height and weight, vital signs, symptoms, and allergies); 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. For instance, personal health data under the DSP includes data regarding U.S. persons' exercise habits collected by fitness apps.

Review of internal datasets and data types is an essential initial step for compliance.

I Am Not a "Data Broker;" Does the DSP Still Apply to Me?

Potentially. Data brokerage is defined as "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." Given this broad definition, many organizations that are not in scope under traditional data broker laws regularly engage in commercial transactions that are considered "data brokerage" under the DSP.

The thresholds for transferring certain categories of sensitive data in "bulk" vary from category to category, as set forth in Table 2. Additionally, thresholds are calculated on a rolling 12-month period, and processing sensitive personal data in "bulk" can be met by a single transaction or aggregated across multiple transactions. Notably, however, for multiple transactions to be aggregated, the transactions must be between the same U.S. person and the same foreign person or covered person.

Category of Sensitive Person	Bulk Threshold (Number of U.S. Persons/Devices)
Human Genomic Data	More than 100
Human Epigenomic, Proteomic & Transcriptomic Data	More than 1,000
Biometric Data	More than 1,000
Personal Health Data	More than 10,000
Combined data, as described in § 202.205(g)	Lowest applicable number

Table 2

I Do Not Transact Business with Companies in the "Countries of Concern" or "Covered Persons"; Do I Still Have Compliance Obligations?

Yes. The DSP prohibits U.S. persons from engaging in data brokerage transactions involving sensitive personal data with countries of concern or covered persons, unless exempt or authorized by a license. Countries of concern are China (including Hong Kong and Macau), North Korea, Cuba, Russia, Iran, and Venezuela. Covered persons are individuals or entities that are subject to the ownership, direction, jurisdiction, or control of a country of concern, or that are designated by DOJ based on certain criteria.

However, even if you are not directly transacting business with the six countries currently enumerated in the DSP or a covered person, under their control, U.S. businesses still have compliance obligations related to *any data brokerage transaction with **any foreign person** that involves bulk U.S. sensitive personal data*. Specifically, in any data brokerage transactions with a foreign person, U.S. persons must:

contractually require the foreign person to refrain from engaging in any subsequent data brokerage transaction involving the same data with a country of concern or covered person;

report any known or suspected violations of this contractual requirement to the DOJ within 14 days of becoming aware or suspecting a violation; and

exercise reasonable and proportionate due diligence to ensure and monitor compliance with the contractual prohibition on onward transfer. This includes developing risk-based compliance programs and monitoring counterparties for compliance.

For example, if a U.S. business licenses data to an Irish company, the data licensing agreement must contractually prohibit the Irish company from subsequently licensing the data to countries of concern or covered persons. Otherwise, it is a prohibited transaction. Additionally, the U.S. business is obligated to conduct due diligence to confirm the Irish company is complying with this contractual obligation, which itself likely also requires specific language to allow for reasonable compliance audits.

The DOJ's guidance documents provide sample contractual language but is clear that the language is not "model" language; the required contractual language should be tailored to the organization's activities and risk profile. Further, U.S. businesses should require that foreign entities provide compliance certifications at appropriate intervals and agree to auditing regarding compliance.

The DSP also restricts U.S. persons from engaging in vendor, employment, or investment agreements that allow countries of concern or covered persons to obtain access to bulk U.S. sensitive personal data unless they comply with certain security requirements (Subpart D), due diligence and audit (Subpart J), and reporting and recordkeeping requirements (Subpart K). If the data involved are bulk human 'omic data – or human biospecimens from which such data can be derived – the transaction is prohibited outright. The Final Rule defines *access* as:

"Logical 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." (§ 202-201)

What Exemptions May Be Applicable to U.S. Health Care and Life Science Organizations?

The DSP provides several exemptions for transactions that are necessary for public health, safety, or welfare, such as:

- Transactions conducted pursuant to a grant, contract, or other agreement with federal departments and agencies, such as the National Institutes of Health, the Food and Drug Administration, or the Centers for Disease Control and Prevention, to conduct and share the results of federally funded research. For example, research projects that receive both federal and non-federal funding are exempt to the extent such transactions are conducted pursuant to a grant, contract, or other agreement with federal departments and agencies.

- Transactions that are ordinarily incident to clinical investigations and post-marketing surveillance, such as sharing data with foreign regulators, investigators, or sponsors for the purposes of obtaining or maintaining marketing authorization, conducting safety monitoring, or reporting adverse events.

- Transactions that are required or authorized by federal law or international agreements, or necessary to comply with federal law.

- Transactions that involve certain drug, biological product, and medical device authorizations, such as sharing data with foreign manufacturers, suppliers, or distributors for the purposes of obtaining or maintaining emergency use authorization, premarket approval, or investigational device exemption.

Health care and life sciences organizations that engage in or contemplate engaging in any of the above transactions should ensure that they meet the criteria and conditions for the applicable exemption and comply with any recordkeeping or reporting requirements that may apply.

Practical Takeaways for Health Care and Life Sciences Organizations:

- **Know your data**: Identify the types and volumes of data that you collect, maintain, process, or transfer about U.S. persons, and whether they fall within the categories of government-related data or bulk U.S. sensitive personal data. Be mindful that, unlike most privacy laws and regulations, the DSP covers data that is anonymized, pseudonymized, de-identified, and/or encrypted. Be aware that the DSP's definition of Protected Health Information is broader than the definition of health information under HIPAA and includes more than just data collected by medical or health care professionals or institutions.

- **Know your transactions**: Identify the transactions that involve access by a country of concern or a covered person to government-related data or bulk U.S. sensitive personal data, and whether they involve data brokerage, vendor agreements, employment agreements, or investment agreements. Be aware that the DSP covers transactions that are commercial in nature, meaning that they involve some payment or other valuable consideration, such as the possibility of research collaboration or co-authorship. Recognize that the DSP prohibits evasions, attempts, causing violations, and conspiracies to violate the DSP's requirements.

- **Know your counterparties**: Identify the parties with whom you engage in data transactions, and whether they are located in, organized under the laws of, or subject to the ownership, direction, jurisdiction, or control of a country of concern, or whether they are designated by the DOJ as covered persons. Screen your vendors, investors, and employees against the Covered Persons List and other relevant lists, and conduct due diligence to verify their identity, ownership, citizenship, residence, and end use of the data. Additionally, be mindful that – even if the counterparty is not a Covered Person – if they are a "foreign entity," you may still need to comply with the DSP depending on the nature of your relationship with them.

- **Know your exemptions and licenses**: Identify the transactions that may be exempt from the DSP's prohibitions or restrictions and ensure that you meet the criteria and conditions for the applicable exemption. Be aware that some exemptions may still require recordkeeping or reporting. If you engage in or contemplate engaging in a transaction that is not exempt and that would otherwise violate the DSP, determine whether you need to apply for a license or seek an advisory opinion. Be advised that there is a presumption of denial standard for license applications, and that licenses may be revoked or modified at any time.

- **Know your compliance program**: Develop, implement, and update a written, risk-based data compliance program that includes policies and procedures for verifying data flows, vendor identity, and end use of the data; implementing security requirements; conducting audits; and complying with all necessary reporting. Training for employees and other personnel is recommended. Review and certify your compliance program and security practices annually. Consult with legal counsel as needed to seek guidance or clarification on the DSP's requirements.

For more information or assistance on this topic, please contact Michael J. Halaiko, Alexandra P. Moylan, Julie A. Kilgore, or another member of Baker Donelson's Health Law team.