bodman

A Health Care Law Update

Bodman PLC **July 10, 2025**

DOJ Data Security Program – Another Privacy and Security Law that Impacts the Health Care Industry

By: Grace A. Connolly (Associate), Annalise Lekas Surnow (Member), and Brandon M. Dalziel (Member and Chair), Health Care Practice Group

The Department of Justice ("DOJ") implemented the Data Security Program ("DSP") intending to prevent access to Americans' bulk sensitive personal data and government-related data by Countries of Concern. The DSP is aimed at addressing national security risks associated with the transfer of sensitive data and information to foreign adversaries, but it may more broadly affect the health care industry. The DSP took effect on April 8, 2025. The DOJ is now fully enforcing DSP following the initial 90-day period of limited enforcement which ended on July 8, 2025.

Any health care organization that is engaged in data brokerage transactions or licensing arrangements may have compliance obligations under DSP. In this Health Care Update, we will review the provisions of DSP and discuss its impact on health care organizations, review compliance obligations and potential consequences of non-compliance, and discuss next steps in DOJ enforcement of DSP.

DSP Regulations and Definitions

The DSP prohibits U.S. entities and individuals from knowingly engaging in "Covered Data Transactions" which include data brokerage, vendor agreements, employment agreements or investment agreements or any other transactions involving access to "Bulk U.S. Sensitive Personal Data" or "Government-related Data" by "Countries of Concern" or "Covered Persons." Countries of Concern include foreign countries that pose a significant risk to U.S. national security, including China, Russia, Iran, North Korea, Cuba, and Venezuela. Covered Persons include foreign entities that are majority-owned by Countries of Concern or have their principal place of business in any Countries of Concern and individuals that are employees or contractors of a Country of Concern or Covered Person or whose primary residence is in a Country of Concern.

The DSP further requires U.S. persons engaging in Covered Data Transactions with any foreign persons (not just Covered Persons) to contractually prohibit such foreign persons from selling or transferring any data to Countries of Concern or Covered Persons and the U.S. person must report any known or suspected violations of this contractual requirement to the National Security Division of the DOJ.

Unlike Health Insurance Portability and Accountability Act ("HIPAA") and other data privacy regulations imposed on the health care industry, "Bulk U.S. Sensitive Personal Data" is defined broadly under the DSP as sensitive personal data relating to U.S. persons in any format and the definition *does not* exclude anonymized, pseudonymized or de-identified data. Such data must also meet certain data-specific thresholds to be considered bulk data (i.e., involving a certain number of U.S. persons, such as biometric identifiers collected on more than 1,000 U.S. persons).

Impact on the Health Care Industry

The DSP covers data typically processed by U.S. health care organizations, including genomic data, biometric data, which includes measurable physical characteristics or behaviors such as facial images or fingerprints, and personal health data, including medical records, test results and immunizations. DOJ guidance confirms that "personal health data" is not limited to Protected Health Information or data collected by Covered Entities as regulated by HIPAA. Rather, "personal health data" is data collected or held by *any entity* that indicates, reveals, or describes the past, present or future physical or mental health condition of an individual, provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual. "Personal health data" includes basic physical measurements and health attributes, such as height, weight, vital signs, allergies etc., treatment history, immunization data and more. The definition even includes data regarding U.S. persons' exercise habits collected by fitness apps.

All U.S. health care organizations – even those that are not directly transacting business with Countries of Concern or Covered Persons - still have compliance obligations related to any data brokerage transaction with any foreign person that involves "Bulk U.S. Sensitive Personal Data." In such transactions, U.S. health care organizations must ensure that: (1) foreign persons refrain from engaging in subsequent data brokerage with Countries of Concern or Covered Persons; (2) they will report any known or suspected violations within 14 days of becoming aware or suspecting a violation; and (3) they will exercise reasonable and proportionate due diligence to ensure and monitor compliance with the contractual prohibition on subsequent data transfers, including the development of risk-based compliance programs.

If an organization is entering into licensing arrangements, it must ensure licensee compliance with the DSP. The grant of any worldwide license rights should not permit any Countries of Concern or Covered Persons to access any data covered by the DSP.

Licensees cannot further license or enter into data brokerage arrangements with any Countries of Concern or Covered Persons.

Consequences to Health Care Organizations for Violations and Compliance Measures

The DOJ can impose steep civil and criminal penalties for non-compliance with the DSP, including fines of up to $368,136 per violation and imprisonment for willful breaches. Given the seriousness of the penalties that may be imposed, prompt compliance remains critical.

To assist with your compliance efforts: (1) assess data license agreements and other agreements to determine whether data covered by the DSP is implicated; (2) assess whether the impacted agreements constitute a prohibited or restricted transaction; and (3) assess whether there is either access by, or any restrictions within the agreements to limit access by, "Countries of Concern", "Covered Persons", or additional restrictions on further access or circulation of data in agreements with any foreign person.

What's Ahead?

During the initial full-enforcement period the DOJ will strictly focus its efforts on compliance with the prohibitions of Prohibited Transactions and limitations on Restricted Transactions. However, beginning October 6, 2025, additional reporting requirements for certain restricted and prohibited transactions will take effect along with due diligence requirements and audit requirements for restricted transactions.

Bodman PLC can provide practical advice on compliance with DSP and any other legal issues affecting your organization. For more information, please contact Brandon Dalziel at (313) 393-7507 or bdalziel@bodmanlaw.com, Annalise Lekas Surnow at (313) 392-1059 or alekas@bodmanlaw.com or Grace Connolly (313)-393-7563 or gconnolly@bodmanlaw.com.

***Bodman cannot respond to your questions or receive information from you without first clearing potential conflicts with other clients. Thank you for your patience and understanding*.**