wiley

ALERT

Personal Health Data at Risk of Foreign Exploitation

February 2, 2022

Issue: The U.S. Government is warning American health care entities that personal health data, including genetic information, from diagnostic tests and services could end up in the hands of foreign governments for unintended purposes if they contract with foreign companies or use overseas facilities. Some of these companies are subject to foreign laws that can compel them to share such data with foreign governments, including governments that exploit personal health data for their own ends without regard to individual privacy.

According to the National Counterintelligence and Security Center (NCSC), several Chinese companies have partnered or contracted with U.S. organizations and are accredited, certified, or licensed to perform genetic testing or whole-genome sequencing on patients in the U.S. healthcare system, potentially giving them direct access to the genetic data of patients in the United States. Chinese companies are compelled to share data with the government of the People's Republic of China, which has used genetic data for state surveillance and repression of its ethnic and religious minorities, as well as for military purposes. This is part of the Chinese government's larger efforts to collect a range of data from foreign persons that may potentially be used as weapons against foreign targets.

What does it mean for the healthcare industry? Health care companies play a significant role in safeguarding the personal health information they collect within the United States since the U.S. does not have a national data privacy and security law which governs the relocation, transfer, and storage of U.S. genetic or other personal health data overseas. Companies should review the privacy and data security policies of the diagnostic testing or services companies they are contracting with to see if they allow for the collection, transfer,

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Jacqueline F. "Lyn" Brown
Partner
202.719.4114
jfbrown@wiley.law

Hon. Nazak Nikakhtar
Partner
202.719.3380
nnikakhtar@wiley.law

Practice Areas

Health Care
National Security
Privacy, Cyber & Data Governance

processing or storage of U.S. patient or consumer data abroad and whether the data may be subject to the laws of foreign nations which might compel sharing.

Companies could end up sharing personal health data, including genetic data with a foreign government for purposes that the patient or consumer never intended. Loss of DNA data to unwanted parties is permanent and can be used by malicious foreign governments to build profiles on individuals for potential surveillance, coercion, or manipulation. Collection of large data sets from around the work by foreign governments can potentially enhance their global market share and economic advantage in pharmaceutical and health care sectors at the expense of U.S. companies.

While U.S. companies performing research through partnerships and data sharing arrangements with foreign companies can result in medical breakthroughs, foreign companies and/or foreign governments collecting U.S. personal health data can also pose risks to individual privacy and U.S. economic and national security as well.

**

What does the U.S. Government warning do?

NCSC is seeking to protect personal health data from foreign exploitation by warning companies about the unintended consequences of contracting with foreign companies or with U.S. companies that have facilities in certain overseas locations which compel data sharing with the government such as China.

Before partnering or contracting with a company that offers diagnostic tests or services in the United States, organizations should examine who they are doing business with and look for any foreign connections. Companies partnering with foreign entities should consider the following risk mitigation measures:

- Review privacy and security policies to determine whether they permit the collection, transfer, processing, or storage of U.S. patient or consumer data abroad.
- Determine the company's potential foreign government ownership or ties.
- Determine if laws in the home country of the company or its affiliates require data sharing with foreign governments.
- Negotiate contracts that require U.S. patient or consumer data to be held in the United States and prohibit that data from being transferred abroad without patient or consumer consent.

If an organization has already partnered or contracted with a company with foreign ties, it should determine the security and privacy impact of the data that has already been shared. Consider the sensitivity of what data has been shared along with the quantity of data that has been shared. Large amounts of seemingly non-sensitive data can be aggregated and the patterns or relationships from that aggregation can be exploited by malicious foreign actors. Companies should ensure that patient or consumer disclosures explain potential security risks and loss of privacy.

Key Takeaways

Wiley has consistently advised of the importance of due diligence when contracting with foreign companies or when doing business in foreign locations. Safeguarding U.S. patient or consumer data from compelled disclosure under foreign laws should be a consideration when U.S. companies execute contracts or enter into partnerships with foreign companies. Wiley can help review a company's proposed contracts or partnerships with foreign entities as well as the privacy and data security policies of the overseas company to spot legal, privacy, or data security issues that require mitigation.