THE NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

SAFEGUARDING OUR FUTURE

Protecting Personal Health Data from Foreign Exploitation

THREAT

Foreign companies and some U.S. businesses with facilities abroad have been partnering or contracting with U.S. organizations to provide diagnostic tests and services that in some cases collect specimens, DNA, fitness / lifestyle information, or other personal health data from patients or consumers in the United States. Some of these companies may be 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 and without regard to individual privacy.

For example, 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.[1] Chinese companies are compelled to share data with the government of the People's Republic of China,[2] which has used genetic data for state surveillance and repression of its ethnic and religious minorities,[3,4] as well as for military research and applications.[5]

Although research performed through partnerships and data sharing with foreign companies can potentially yield medical breakthroughs,[6] the collection of U.S. personal health data by foreign companies can also pose potential risks to individual privacy and U.S. economic and national security.

RISKS

Privacy: Your personal health data, including genetic data, could end up in the hands of a foreign regime and used for purposes you never intended. Loss of your DNA to unwanted parties is permanent and not only affects you, but also your relatives, and potentially future generations.

Intelligence: Foreign regimes can combine personal health data, including genetic data, with other personal data sets they have collected to build profiles on individuals for potential surveillance, coercion, or manipulation.

Economic: Collection of large, diverse genomic data sets from around the world by foreign regimes and companies can boost their global market share and economic advantage in pharmaceutical and health care sectors at the expense of U.S. commercial health and research sectors when there is no reciprocal sharing of health data by the foreign entities.

Military: Foreign regimes can use large, diverse genomic data sets from around the world for military-related research, including biodefense.

SAFEGUARDING OUR FUTURE

Protecting Personal Health Data from Foreign Exploitation

MITIGATION FOR U.S. ORGANIZATIONS

- Before partnering or contracting with a company that offers low-cost diagnostic tests or services in the United States, know who you are doing business with and identify any foreign connections.
  - Review their privacy and data security policies to determine if they allow for the collection, transfer, processing, or storage of U.S. patient or consumer data abroad.
  - Determine the company's potential foreign government ownership or ties, as well as contractual and legal obligations. Determine if laws in the home country of the company or its affiliates require data sharing with foreign governments.
  - Consider whether the risks of a foreign government gaining access to U.S. patient or consumer data outweigh the potential cost savings of contracting with the company.
  - 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.
  - Set security and privacy standards for the company's handling of U.S. patient or consumer data and continuously monitor compliance.

- If you already have partnered or contracted with the company, ascertain the security and privacy impact of data shared. Consider not only the sensitivity of the data shared, but also the quantity. Large sets of seemingly non-sensitive data can be aggregated for the identification of patterns or relationships and be exploited.
  - Provide patient or consumer disclosures that enumerate potential security risks and loss of privacy.
- Maintain enduring connectivity to the U.S. Government for the latest threat information and security best practices.
  - General NCSC resources are available at www.ncsc.gov. NCSC's February 2021 bulletin on threats to U.S. genomic data can be found here, while NCSC's supply chain risk management resources can be found here.

MITIGATION FOR U.S. PATIENTS OR CONSUMERS

- Understand you have a significant role in safeguarding your data, as there is not a comprehensive, national U.S. data privacy and security law that governs the relocation, transfer, and storage of U.S. genetic or other personal health data overseas.
- Know your rights. Ask questions and take time to read the fine print before providing consent to turn over your personal health data, including genetic, medical, fitness, and lifestyle data.
- Review the privacy and data security policies of the diagnostic testing or services company to determine if they allow for the collection, transfer, processing, or storage of U.S. patient or consumer data abroad and whether that data may be subject to the laws of foreign nations.

---

[1] "China's Biotechnology Development: The Role of US and Other Foreign Engagement," A report prepared by Gryphon Scientific, LLC, and the Rhodium Group, LLC for the U.S.-China Economic and Security Review Commission, February 14, 2019, pp. 122, 124.
[2] Annual Threat Assessment of the U.S. Intelligence Community, Office of the Director of National Intelligence, April 9, 2021, pg. 20.
[3] "Commerce Department Adds Eleven Chinese Entities Implicated in Human Rights Abuses in Xinjiang to the Entity List," U.S. Department of Commerce press release, July 20, 2020.
[4] Xinjiang Supply Chain Business Advisory, "Risks and Considerations for Businesses and Individuals with Exposure to Entities Engaged in Forced Labor and other Human Rights Abuses linked to Xinjiang, China," U.S. Department of State, U.S. Department of Treasury, U.S. Department of Homeland Security, Office of the U.S. Trade Representative, U.S. Department of Labor, Updated July 13, 2021, pg. 4.
[5] "Commerce Acts to Deter Misuse of Biotechnology, Other U.S. Technologies by the People's Republic of China to Support Surveillance and Military Modernization that Threaten National Security," U.S. Department of Commerce press release, December 16, 2021.
[6] "China's Biotechnology Development: The Role of US and Other Foreign Engagement," A report prepared by Gryphon Scientific, LLC, and the Rhodium Group, LLC for the U.S.-China Economic and Security Review Commission, February 14, 2019, pg. 122.