COSMOS
Navigate the Compliance Universe

Compliance Today - May 2021
Healthcare data as a national security concern

By Angela Gamalski, JD, MHSA, CHC

Angela Gamalski (agamalski@honigman.com) is an Associate at Honigman LLP in Detroit, MI.

- linkedin.com/in/angelaigamalski/

Companies operating in the healthcare industry may hold sensitive healthcare and financial data for thousands or millions of individuals. While specific healthcare data are protected by certain privacy requirements (e.g., the Health Insurance Portability and Accountability Act (HIPAA) of 1996, as amended), this broader set of sensitive individual data is also a target for national security concerns, and as such, the risk of compromise should be evaluated and appropriate security and compliance measures enacted.

As this article will explain, routine business transactions, management changes, or investments can be subject to review by the US government for national security purposes if such sensitive individual data are at stake and non-US companies or individuals are involved. Compliance and privacy professionals should understand how these risks apply to their business and work with governance and compliance stakeholders to address these risks.

Background regarding national security transaction reviews

The Exon–Florio Amendments of 1988 first established the Committee on Foreign Investment in the United States (CFIUS) as an interagency committee empowered to review business transactions involving foreign companies acquiring sensitive or otherwise valuable US companies.[1] Twenty years later, the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) yielded the first major regulatory overhaul of CFIUS and expanded its authority as to the types of transactions that could be reviewed as well as mandating review for certain types of transactions.[2] The CFIUS review process looks to understand the threat posed to national security by a foreign person, the extent to which a particular US business can influence national security, and potential national security issues that could be exploited as a consequence of a particular business transaction.

CFIUS is authorized to review a variety of transactions, including any merger, acquisition, partnership, joint venture, investment, or takeover by or with a foreign person that could result in foreign control of a US business; foreign access to information in the possession of, rights in, or involvement in the substantive decision-making of certain US businesses related to critical technologies, critical infrastructure, or sensitive personal data; or foreign ownership of property in close proximity to sensitive or strategic US locations. While CFIUS review is generally voluntary, CFIUS is also authorized to review any transaction involving foreign buyers that was not submitted for notice or any other transaction, transfer, agreement, or arrangement that was structured to evade or circumvent CFIUS authority. Failing to obtain a CFIUS review when such review was required can result in significant penalties, up to the value of a business transaction, and/or the unwinding of a deal (even years after the fact).

Whether a buyer or investor is deemed to be a foreign person is a fact-based analysis that considers the nationalities of the person or entity who is making the purchase or investment. In the case of a business entity, the analysis also considers the nationalities of those who control the business, whether the entity is backed by a

foreign government, and other shareholder arrangements between the parties who comprise the entity.[3] While FIRRMA establishes a threshold investment amount for passive investment transactions, any investment equity interest with control or information rights is subject to scrutiny.[4] CFIUS has broad authority, and any scenario in which ownership, control, or information rights are granted to or could be asserted by a non-US person or entity, through management arrangements or significant customer or vendor relationships, could be the subject of CFIUS review.

CFIUS reviews target healthcare data

Certain types of businesses have mandated CFIUS reviews, defined as technology, infrastructure, and data businesses.[5] Under the Department of the Treasury regulations, sensitive personal data are identifiable data maintained or collected by a US company for more than one million individuals over a 12-month period and include, but are not limited to, financial data that could be used to determine an individual's financial distress or hardship; data relating to the physical, mental, or psychological health condition of an individual; and biometric enrollment data.[6] Notably, these various types of data can be aggregated for purposes of determining whether a company's data troves cross the one-million-individual threshold, and also include all data that may be currently retained from past customers if subject to a lengthy data retention policy. Adherence to current industry data protection standards, such as the National Institute of Standards and Technology or International Organization for Standardization frameworks (colloquially known as NIST and ISO, respectively), is not enough to categorically exempt a business from CFIUS review.

One of the most public review processes in recent years was that which occurred for TikTok, the social media app owned by ByteDance, a Chinese company. In August 2020, the US government ordered that TikTok's assets be sold to a US company to protect the security of its user data.[7] Notably, the TikTok order came despite a number of mitigation strategies to protect user data, but this order was not an unprecedented action. CFIUS has previously stepped in to unwind transactions that involved social media, sensitive data, and foreign investors. For example, CFIUS blocked a foreign investment in a healthcare social media company called PatientsLikeMe.[8] CFIUS is staffed by civil servants, not political appointees, so its trajectory is unlikely to change under a new administration. Therefore, these examples have implications for healthcare privacy and compliance professionals.

Like so many government processes, CFIUS reviews consider the strength of a company's compliance program. Compliance professionals are well positioned to understand the significance of the sensitive individual data held by their company, which for CFIUS purposes extend well beyond protected health information. First and foremost, a risk analysis of the sensitive individual data and operational data framework is essential. A cross-sectional compliance committee or work group should be assembled to understand whether security protections and access restrictions are in place as part of routine business practices, who within a company can reach the fully identifiable data stored, and the data retention periods required for all forms of such information. Moreover, when a company is considering new business ventures, compliance professionals should be part of the business negotiations and can provide input as to what information will be exchanged, by what mechanisms, and how access will be controlled.

Proposed commerce rules for high-tech software and hardware

The U.S. Department of Commerce (Commerce) will now have responsibility for review and control of certain imports of software and hardware source code or designs made by foreign persons from certain designated countries. In January, Commerce proposed broad regulations to secure the information and communications

technology and services (ICTS) supply chain of software and hardware that support or are integral to network management, data storage, and internet-connected devices (the ICTS rules).[9] The ICTS rules will build on Executive Order No. 13873, issued May 15, 2019.[10] At the time this article went to press, the Biden administration had placed these outgoing Trump administration actions under administrative review.[11] While the new administration's review may result in some modifications to the language and implementation time frame for the final ICTS rules, the ICTS rules reflect longstanding national security concerns and align with other established regulatory regimes, as discussed in this article and elsewhere.[12] Thus, the major themes highlighted here are likely to remain amid any regulatory evolution that may take place.

The ICTS rules establish a process for Commerce to review a vast range of ongoing business activities, including any purchase, import, transfer, installation, dealing in, or use of a technology or service, including managed services, software updates, and download hosting services of ICTS (each, an ICTS transaction).[13] An ICTS transaction involving any ICTS produced by any person or company owned by, controlled by, or subject to the jurisdiction or direction of certain designated countries and regions, which are Russia, China and Hong Kong, Cuba, Iran, North Korea, and the Maduro Regime of Venezuela, will be subject to mandatory Commerce review (a covered ICTS transaction).

Covered ICTS transactions include integral hardware or software sourced from the above-listed countries and used by critical infrastructure sectors designated under Presidential Policy Directive 21, released February 12, 2013.[14] The healthcare and public health critical infrastructure sectors include private direct patient care, health information technology, health plans and payers, medical materials, laboratories, blood, and pharmaceuticals.[15] A covered ICTS transaction also includes the following: wireless or mobile networking equipment, hosting sensitive individual data of more than one million Americans annually, and an internet connectivity device or service used by more than one million Americans annually.[16] While Commerce has not yet issued its complete guidance on the ICTS rules, the CFIUS guidance above relative to data retention policies or the aggregated data types held should be informative, as it may cause a transaction to become a covered ICTS transaction.

As currently written, covered ICTS transactions will be subject to mandatory Commerce review, and any party involved in the acquisition of covered ICTS can be included in this review.[17] Review standards will look to numerous factors, including facts and circumstances regarding the parties and foreign governments involved in the design, development, manufacture, and supply of the ICTS at issue; the parties to the ICTS transaction; the nature of the vulnerabilities implicated by the ICTS transition; the ability of the parties to mitigate transaction risk; the severity and likelihood of potential harm posed to health, safety, and security; the critical infrastructure; and sensitive data (among others).[18] Companies or individuals that violate the ICTS rules, whether by failing to submit for review of a mandatory covered ICTS transaction or maintain mitigation requirements set forth by Commerce, may be liable for civil or criminal penalties under federal national security laws.[19]

Compliance action steps

Companies in the healthcare industry are targeted by these regulations for holding sensitive individual data, including protected health information, as a necessary component of the healthcare business. Compliance professionals are best positioned to understand the risks unique to their businesses and to advocate for resources to support areas, such as cybersecurity, that would be scrutinized under either of these review regimes. Under either review regime, the government will scrutinize a company's culture of compliance (or lack thereof) and the

strength of the company's policies, procedures, and security posturing to protect sensitive individual data.

Now more than ever it is critical to understand who makes the goods; who produces the services the company is purchasing; whether there are additional downstream vendors in the supply chain; and how those goods or services connect to, store, or support sensitive individual data. Compliance professionals should investigate whether supply chain due diligence considers foreign ownership and affiliate relationships as part of the vendor screening processes, as well as from where and from whom those vendors are sourcing critical components, the business partners the vendor may be working with, and the upstream ownership of those entities if publicly available.

The CFIUS review process and other national security laws may largely operate in the background and outside of the day-to-day concerns of many entities in the healthcare industry. In particular, the ICTS rules have not been fully promulgated, and the full meaning and requirements of these rules have not yet been laid out. During this unprecedented age of COVID-19, and as vaccine passports loom on the horizon, entities considering new collaborative projects with international partners would be wise to establish processes now that effectively screen counterparties, and compliance professionals can help facilitate these types of discussions. Foreign investments in healthcare suppliers may get additional CFIUS scrutiny in a post-COVID-19 world, while the ICTS rules will most likely affect the sourcing decisions and customer diligence process.

Takeaways

- Business transactions or investments involving non-US entities are subject to review by the US government for national security purposes.
- Companies operating in the healthcare space that have access to sensitive personal data, including healthcare data, are subject to this review process, which can encompass all information about the parties at the government's disposal.
- Information technology goods sourced from China and other countries are now subject to review by the U.S. Department of Commerce for national security concerns, and healthcare data companies are defined as a critical industry for such review.
- These laws may not affect the day-to-day operations of most companies, but the government authority to review business activities and transactions is largely unlimited without any statute of limitations.
- Foreign investments in healthcare suppliers may get additional scrutiny in a post-COVID-19 world, while the final information and communications technology and services rule to be issued by the Department of Commerce will most likely affect the sourcing decisions and customer diligence process.

1 50 U.S.C. app. § 2170.
2 Foreign Investment Risk Review Modernization Act of 2018, Pub. L. No. 115-232, §§ 1701–1728, 132 Stat. 2173 (codified as amended in scattered sections of 50 U.S.C.).
3 31 C.F.R. §§ 800.214–800.215, 800 .241.
4 31 C.F.R. § 800.241 .
5 31 C.F.R. §§ 800.214–800.215, 800 .241.
6 31 C.F.R. § 800.241 .
7 Addressing the Threat Posed by TikTok, and Taking Additional Steps To Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain, 85 Fed. Reg. 48,637

(August 11, 2020) , https://bit.ly/2P10VGE.
8 Jeff Farrah, "Another day, another US company forced to divest of Chinese investors," *TechCrunch*, April 15, 2019, http://tcrn.ch/38R3kYB.
9 Securing the Information and Communications Technology and Services Supply Chain, 86 Fed. Reg. 4,909 (January 19, 2021) .
10 Executive Order 13873 of May 15, 2019, 84 Fed. Reg. 22,689 (May 17, 2019) , https://bit.ly/31bvVDT.
11 Ronald A. Klain, "Regulatory Freeze Pending Review," memorandum for the heads of executive departments and agencies, January 20, 2021, https://bit.ly/304l737.
12 Soniya Shah, "The Problem with Foreign Investment: Using CFIUS & FIRRMA to Prevent Unauthorized Foreign Access to Intellectual Property," *Administrative Law Review Accord* 6, no. 1 (September 2, 2020), https://bit.ly/3qZ0IOo.
13 Securing the Information and Communications Technology and Services Supply Chain, 86 Fed. Reg. 4,909 .
14 The White House, "Presidential Policy Directive -- Critical Infrastructure Security and Resilience," news release, February 12, 2013, http://bit.ly/380i4Y8.
15 U.S. Departments of Homeland Security and Health & Human Services, *Healthcare and Public Health Sector-Specific Plan*, May 2016, 5, https://bit.ly/3vvrKjY.
16 Securing the Information and Communications Technology and Services Supply Chain, 86 Fed. Reg. 4,924 .
17 Securing the Information and Communications Technology and Services Supply Chain, 86 Fed. Reg. 4,925 .
18 Securing the Information and Communications Technology and Services Supply Chain, 86 Fed. Reg. 4,927 .
19 Securing the Information and Communications Technology and Services Supply Chain, 86 Fed. Reg. 4,919 .