Health-ISAC Weekly Blog -- Hacking Healthcare™

Hacking Healthcare™ | TLP:WHITE | Alert ID : 4d0277c8 | Aug 03, 2023, 08:31 AM

This week, *Hacking Healthcare*™ examines what the totality of recent Chinese cybersecurity, privacy, and counter-espionage laws and regulations means for the healthcare sector. We identify some of the more significant legislation that has been passed to increase government oversight of foreign organizations, outline the risks they create for healthcare organizations, and provide some recommendations on how to mitigate those risks.

China: Oversight of Industry

Over the past decade, the People's Republic of China (PRC) has increasingly passed legislation to expand governmental oversight on domestic and foreign companies operating within its borders. This legislation appears part of a broader trend by the PRC to improve its ability to monitor and control data flows and information that may impact its strategic goals and national security. Despite not specifically targeting healthcare entities, many of these laws, and the overall trend they create, may affect healthcare entities in several direct and indirect ways that are worth considering.

Since 2015, a series of laws have been passed by the PRC that have had significant implications for the cybersecurity and privacy of data stored or processed in China, and data transmitted to or out of the country. These laws have included things like requiring organizations to report cybersecurity vulnerabilities to the PRC before anyone else, expanding the definition of espionage to encompass a vague and broad range of activities, and requiring Chinese citizens, including those working for multinational organizations, to assist in government intelligence efforts.

Below is a brief overview of the more prominent laws whose impacts we will investigate in the analysis section.

2017 Cybersecurity Law (CSL) mandates that critical infrastructure companies must retain their data within the PRC's borders and requires that the stored data be made accessible to its intelligence services. As a result, companies must localize certain types of data within China, including foreign companies' data working in undefined critical industries.[i] This law is targeted towards service providers and network operators and sets strict guidelines for managing cybersecurity incidents.[ii]

2017 National Intelligence Law states that citizens or private organizations must play a role in assisting the Ministries of Public Security and State Security in their national intelligence efforts.[iii] The law stipulates legal responsibilities for both Chinese and foreign entities to provide access to and collaborate with Chinese intelligence agency initiatives, and provides legal grounds to monitor and investigate foreign and domestic individuals and bodies for the purposes of national security.[iv]

2021 Data Security Law (DSL) classifies data in a tiered system according its importance to state security, imposes additional regulatory requirements on cross-border data flows, and grants the government the power to deny data transfers and refuse foreign government data transfer requests. The DSL applies widely, impacting almost every organization conducting business within China, but notably it tightens the restrictions on transfers of data outside China. Specifically, it prohibits provision of any data stored in China, regardless of its classification level, to any foreign judicial or law enforcement agency without the prior approval of a governmental authority.[v]

2021 Personal Information Protection Law (PIPL) codifies the privacy rights of the PRC citizens and requires domestic and foreign companies to comply with the set of regulations.[vi] The PIPL has

extraterritorial effects which limit the collection of data on Chinese citizens within China and abroad, and applies restrictions on the transfer of personal information to third parties and overseas.

2023 Counter-Espionage Law Update broadens the definition of espionage activities "from covering state secrets and intelligence to any documents, data, materials, or items related to national security interests, without defining terms."[vii] The expanded scope and limited specificity within the text makes it difficult to ascertain exactly what might constitute a restricted activity and the uncertainty increases the legal risks for entities, especially foreign entities.

Multinational companies dealing with the collection and cross-border transfer of local data will be impacted by these updates and will need to be vigilant with their data compliance methods.

Action & Analysis
Included with Health-ISAC Membership*

Congress
Tuesday, August 1
No relevant hearings

Wednesday, August 2
No relevant meetings

Thursday, August 3
No relevant meetings

International Hearings/Meetings
No relevant meetings
EU

[i]https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/FINAL_NCSC_SOF_Bulletin_PRC_Laws.pdf
[ii]www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2022/Jan/cted_trends_report_lawful_access_to_digital_data_.pdf
[iii]https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/FINAL_NCSC_SOF_Bulletin_PRC_Laws.pdf
[iv] https://www.reuters.com/article/us-china-security-lawmaking/china-passes-tough-new-intelligence-law-idUSKBN19I1FW
[v]www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2022/Jan/cted_trends_report_lawful_access_to_digital_data_.pdf
[vi]https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/FINAL_NCSC_SOF_Bulletin_PRC_Laws.pdf
[vii]https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/FINAL_NCSC_SOF_Bulletin_PRC_Laws.pdf
[viii] https://www.wsj.com/articles/in-china-a-detention-and-a-new-espionage-law-have-businesses-worried-78fc88b1
[ix] https://www.ft.com/content/4fb65320-3c6a-4a8a-a56a-89a5cb40e069
[x] https://carnegieendowment.org/2022/04/25/countering-unfair-chinese-economic-practices-and-intellectual-property-theft-pub-86925
[xi] https://www.cbsnews.com/news/chinese-hackers-took-trillions-in-intellectual-property-from-about-30-multinational-companies/
[xii] https://www.crx2.org/resources/2019/3/11/on-letting-go-2tx57

Report Source(s)
Health-ISAC

Release Date
Aug 03, 2023, 11:59 PM

Reference | References
CBS News

Wall Street Journal
crx2
Health-ISAC
Financial Times
dni
carnegieendowment
Reuters

Tags

data localization, Hacking Healthcare, Information Sharing, Data Transfer, China

---

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions and/or Comments:

Please email us at contact@h-isac.org

Conferences, Webinars, and Summits:

https://h-isac.org/events/

Hacking Healthcare:

Written by John Banghart, who served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Council's efforts to address significant cybersecurity incidents, including those at OPM and the White House. John is currently the Senior Director of Cybersecurity Services at Venable. His background includes serving as the National Security Council's Director for Federal Cybersecurity, as Senior Cybersecurity Advisor for the Centers for Medicare and Medicaid Services, as a cybersecurity researcher and policy expert at the National Institute of Standards and Technology (NIST), and in the Office of the Undersecretary of Commerce for Standards and Technology.
John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.

Access the Health-ISAC Intelligence Portal:

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

For Questions or Comments:

Please email us at toc@h-isac.org