HACKING HEALTHCARE

Hacking Healthcare - Weekly Blog

 TLP:WHITE

Dec 04, 2025

This week, Health-ISAC®'s Hacking Healthcare® Hacking Healthcare examines newly amended provisions to China's Cybersecurity Law. We identify some of the most significant impacts the new amendments will have, identify who should be paying attention to them, and finish with some specific considerations for Health-ISAC members.

Welcome back to Hacking Healthcare®.

Amendments to China's 2017 Cybersecurity Law

For the first time since going into effect in June of 2017, China's foundational Cybersecurity Law is being amended. Where the original law established the People's Republic of China's (PRC) legal framework governing online activities, data handling, and network security, the new amendments lean into expanding Chinese Communist Party (CCP) control, heightening enforcement powers and extraterritorial reach, and strengthening the alignment between cybersecurity and Chinese national security policy.

Significant Provisions and Issue Areas

- **Party Control and Oversight:** With a one-party system, laws and regulations in China are generally bent towards alignment

with the ruling CCP's general strategic goals and objectives. The recent amendments to the 2017 Cybersecurity Law further solidify that reality by ensuring that compliance with the law aligns with party policy and the security apparatus.

It is notable how explicitly this is being done, as this will be the first time that the legislation formally codifies CCP leadership into the statute. It embeds "the leadership of the Communist Party of China" into the law, requiring all cybersecurity work to "implement the overall national security concept, coordinate development and security, and promote the construction of a cyber power."[i] Additionally, the new Article 30 states that "network operators shall provide technical support and assistance to the public security authorities and state security authorities in lawfully safeguarding national security and investigating crimes."[ii]

As a result, companies covered under the law may find they are at even more of an increased risk of CCP-led oversight and data access expectations than they were previously.

- **Scope of Covered Entities:** The newly amended Cybersecurity Law covers a wide swath of entities thanks in part to a very broad existing definition of the term "Network Operator" which essentially puts in scope nearly all entities that "build, operate, maintain, or use networks" in China. Those operators who handle personal data will now also be required to comply with the Civil Code and the Personal Information Protection Law (PIPL). By linking cybersecurity duties to the PIPL, the PRC has closed gaps between privacy protection and network control, effectively merging data compliance with national security oversight.

- **Critical Information Infrastructure Protections:** For entities judged to be critical information infrastructure, further cybersecurity and data protection measures will now be required. These include data localization elements, third-party assessments, and national security reviews. While the law does not specify the health sector explicitly in the way it does energy, finance, and water, the definition is left open ended to potentially include "other important industries and fields and other critical information infrastructure that will result in serious

damage to the national security, national economy and peoples' livelihood and public interests...".[iii] It would not appear to be unlikely for the health sector to be covered in some manner.

- **Artificial Intelligence:** There is a dedicated AI provision in the amendment which signals that AI systems are now part of the national cybersecurity regime. It allows the state to regulate algorithmic systems and their training data under cybersecurity oversight.

- **Non-compliance Penalties:** Overall, the new amendment increases maximum penalties and adds new penalties for non-compliance. The new penalty structure is tiered, proportional to severity, and harmonized with the Data Security Law and PIPL. It formalizes broad administrative discretion – allowing regulators to suspend, revoke, or shut down noncompliant operations.

- **Extraterritorial Reach:** Article 77 of the newly amended Cybersecurity Law states that "Any foreign institution, organization, or individual who engages in any activity that endangers the cybersecurity of the People's Republic of China shall be held legally liable."[iv] This is an expansion of the 2017 law which initially only covered critical information infrastructure. In effect, this provision could be applied broadly to any instance deemed to have negatively impacted China's cybersecurity. As an example, this could potentially cover vulnerability reporting that prioritizes or engages with entities other than CCP entities. As a result, this provision enables enforcement actions beyond China's borders against entities or individuals perceived as threatening state interests – a relevant risk for companies with China operations or conducting activities that could be perceived by the PRC as hostile.

Action & Analysis

Included with Health-ISAC Membership

[i] *Lexis Nexis Translation of Cybersecurity Law of the People's Republic of China (Amended in 2025)*
[ii] *Lexis Nexis Translation of Cybersecurity Law of the People's Republic of China (Amended in 2025)*
[iii] *Lexis Nexis Translation of Cybersecurity Law of the People's Republic of China (Amended in 2025)*
[iv] *Lexis Nexis Translation of Cybersecurity Law of the People's Republic of China (Amended in 2025)*

Report Source(s)	Health-ISAC

Alert ID 2c67d087

View Alert

Share Feedback
was this helpful? |

Tags cybersecurity law, Regulation, Critical Infrastructure, Security, China

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

Conferences, Webinars, and Summits

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

Hacking Healthcare

Hacking Healthcare is co-written by John Banghart and Tim McGiff.

John Banghart has served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Councils 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 Councils 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.

Tim McGiff is currently a Cybersecurity Services Program Manager at Venable, where he coordinates the Health-ISACs annual Hobby Exercise and provides legal and regulatory updates for the Health-ISACs monthly Threat Briefing.

- John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.
- Tim can be reached at tmcgiff@venable.com.

Access the Health-ISAC Threat 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 Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**