New China rules for cybersecurity for hospitals and clinics

October 2022

Executive summary

The *Healthcare Institutions Cybersecurity Regulation* (issued and effective on 8 August, 2022) (the '**Regulation**') is a new sector specific cybersecurity regulation with which hospitals and clinics operating in China must comply.

The Regulation is one of a number of new data and cybersecurity rules applicable to the pharmaceutical, biotech and healthcare industry which have been issued by Chinese regulators this year, including the *Cybersecurity Review Measures*[1] and the *Measures on Security Assessment of Cross-border Data Transfer*[2]. Consultation papers have also been issued by Chinese regulators in relation to the *Implementation Regulation to the Rules on Human Genetic Resources Administration* and amendments to the *Cybersecurity Law* (to increase the penalties for individuals and companies). These law and regulation are expected to be formally adopted soon.

This article highlights some of the new requirements contained in the Regulation, including a significant number of specific legal obligations. In particular, the Regulation incorporates many elements of the MLPS 2.0 standards (as further described below). Furthermore, the outbound transfer of data requirement set out in the Regulation is stricter than the requirements contained in the China Cybersecurity Law, Data Security Law and Personal Information Protection Law.

Companies in the life sciences industry which are operating in, or considering expanding into, China should evaluate the Regulations and get prepared.

What does the new regulation apply to?

The new Regulation applies to clinical, scientific, management and other business data, data generated by medical devices, personal data and data derivatives, as well as other electronic data which healthcare institutions collect, store, transmit, process or generate.

Liability standard

The new Regulation requires that cybersecurity responsibility should be clearly allocated following the principle of:

'*those who manage the business must also manage cybersecurity, and those who are in management, those who lead operations and those who use the systems are responsible for network security*'.

[1] Effective on 15 February, 2022, and setting out the Chinese government approval requirement governing the procurement of network products or services by life sciences companies which are Critical Information Infrastructure operators.
[2] Effective on 1 September, 2022, and setting out the Chinese government approval process for outbound transfer of certain data (including personal data exceeding the prescribed volume or any volume of Important Data).

The Regulation prescribes that healthcare institutions are the primary responsible parties, and that they must document in writing the respective cybersecurity responsibilities when working with other parties (such as parties involved in the construction of their information technology systems and medical device manufacturers and businesses). the cybersecurity responsibilities when working with other parties (such as parties involved in the construction of their information technology systems and medical device manufacturers and businesses).

Network

The Regulation requires all healthcare institutions to set up cybersecurity leadership groups, which must be led by top management and meet at least once a year to deploy security priorities and implement the *Regulations on the Security Protection of Critical Information Infrastructure* and Multi-level Protection Scheme ('**MLPS**'[3]) requirements. Healthcare institutions of MLPS level 2 or above must allocate cybersecurity responsibility to specific departments and individuals, establish cybersecurity management systems, strengthen cybersecurity protection, and strengthen incident response systems.

All healthcare institutions are specifically required to specify the responsibility of the different departments and the users and comply with the following requirements:

(1) for new networks, the MLPS levels should be determined in the planning stage and submitted to the relevant supervisory authorities for review and approval. All healthcare institutions should review all of their networks, especially cloud computing, Internet of Things, blockchain, 5G, big data and other new technology applications, and determine their MLPS levels based on the functions, service scopes, service objects, data processing, etc., as well as the MLPS standards.

(2) the new networks go live in accordance with legal (MLPS) requirements. Networks which are MLPS level 2 or above should be recorded with the local public security bureaux as well as the supervisory public health authorities within ten working days after the determination of the MLPS levels. In case of change, re-recordals should be proceeded with within ten working days.

(3) all healthcare institutions must review their cybersecurity needs, develop overall construction plans in accordance with MLPS requirements, strengthen security management for both information system development and outsourcing, carry out cybersecurity construction, and implement security protection measures.

(4) each MLPS graded healthcare institution should conduct assessment. Networks of MLPS level 3 or 4 must commission MLPS institutes to carry out MLPS assessment at least once a year. Networks of MLPS level 2 must commission MLPS institutes to regularly carry out MLPS assessments. An MLPS assessment must be carried out at least once every three years for networks handling personal data of more than 100,000 individuals and at least once every five years for all other networks. Newly built networks of healthcare institutions should be tested before going live.

Healthcare institutions which are Critical Information Infrastructure ('**CII**'[4]) operators are required to conduct background checks on key employees for cybersecurity purposes. All healthcare institutions must strengthen controls over internal personnel as well as third parties who handle work relating to the network, including implementing approval processes for accessing the network, enforcing the real-name registration process, conducting background checks on relevant individuals, entering into confidentiality agreements with relevant individuals, etc., and procure only secure network products and services.

All healthcare institutions are specifically required to strengthen operation continuity capability, and the networks of healthcare institutions graded MLPS level 3 or above should ensure strengthened protection for the key links and an abundance of key equipment.

The Regulation requires that the cybersecurity budget for new information technology projects may not be less than 5% of the total project budget.

---

[3] MLPS is China's cybersecurity standard. Under MLPS, companies must conduct assessments of their information systems and the risks associated with them. MLPS has five network security levels based on the damage that would be caused to national security, social order, or public interest in the event of network disruptions or cybersecurity incidents. Each information system is assigned a 'level' based on the importance of the system and data and the potential impact in case of damage. Companies must perform their cybersecurity protection obligations in accordance with the requirements of MLPS. China has updated its MLPS cybersecurity standards and refers to the updated MLPS system as MLPS 2.0.

[4] Critical Information Infrastructure is defined as important network facilities and information systems in the industries of public communication and information services, energy, transportation, water conservancy, finance, public services, e-government, national defence, science and technology as well as those that may seriously endanger national security, national economy and the people's livelihood, and public interests in case of damage, loss of function or data leakage. Industry regulators are responsible for giving guidance and issuing detailed catalogues of CIIs within their own industries.

Data

Healthcare institutions which are CII operators are required to draw up security protection plans, and establish protection systems for data and personal information security.

All healthcare institutions are required to establish organisational structures for data security, specify the data security responsibilities of the operation departments and management departments, systemise and document the rights and responsibilities of the different data management departments for the whole data life cycle, and enforce the system of responsibility.

In addition, all healthcare institutions are specifically required to annually conduct comprehensive reviews of their data assets, update their data security management systems at least once a year, and conduct annual data security risk assessment. (It is recommended that the relevant personnel should sign confidentiality agreements every year.)

All data processing should take place in China and outbound provision of data should only take place if there is an operation necessity, in which case, the outbound provision must comply with the relevant legal requirements (for example, obtaining Chinese government approval in cases of outbound transfer of personal data exceeding the prescribing volume or outbound transfer of important data[5]).

Penalties for non-compliance

Companies can expect the current increased regulatory oversight to continue and intensify as the laws provide regulatory authorities with more explicit and wider monitoring, investigative, and enforcement powers. Companies are required to cooperate with the Chinese authorities. Failure to cooperate with the authorities may result in penalties against the companies as well as the responsible individuals.

Non-compliance will trigger a wide range of potential penalties for companies, including warnings, fines, suspension of operations and imprisonment. The proposed amendments to the Cybersecurity Law increase the fines against companies to as high as RMB 50 million or 5% of turnover of the previous year, and fines of up to RMB1 million against individuals. In addition, individuals may be blacklisted from holding important positions for a certain period of time. The Cybersecurity Law also imposes penalties (such as the freezing of assets) against foreign organisations or individuals who attack or otherwise endanger China's CII.

[5] Important Data are defined as data that may endanger national security, economic operation, social stability, public health, and safety once they are tampered with, destroyed, leaked, or illegally obtained or used illegally.

Let's talk

For a deeper discussion of how this impacts your business, please contact us.

Jan-Peter Ohrtmann
Cybersecurity & Data Protection Leader, Global Legal Network
PwC Germany
+49 (211) 981 2572
jan-peter.ohrtmann@pwc.com

Chiang Ling Li
Partner
Tiang & Partners
+852 2833 4938
chiang.ling.li@tiangandpartners.com

Jay Cline
US Privacy Leader, Principal
PwC US
+1 (763) 498 2237
jay.cline@pwc.com

Nalneesh Gaur
Principal
PwC US
+1 (214) 649 1261
nalneesh.gaur@pwc.com

Joseph Nocera
Cyber & Privacy Innovation Institute Leader
PwC US
+1 (312) 925 6569
joseph.nocera@pwc.com

Mir Kashifuddin
Principal, Cyber, Risk & Regulatory
PwC US
+1 (817) 683 8296
mir.kashifuddin@pwc.com

Robbie Higgins
Principal, Information Technology
PwC US
robbie.higgins@pwc.com

Glenn Hunzinger
Partner, Pharmaceutical and Life Sciences Consulting Solutions Leader
PwC US
glenn.hunzinger@pwc.com

Fedelma Good
Director, Co-lead Data Protection in Legal Business Solutions
PwC UK
+44 (0) 7730 598342
fedelma.good@pwc.com

Chris Cartmell
Director (Solicitor), Co-lead Data Protection in Legal Business Solutions
PwC UK
+44 (0) 7483 353965
chris.cartmell@pwc.com

Pascal Tops
Partner
PwC Belgium
+32 473 91 03 68
pascal.tops@pwc.com

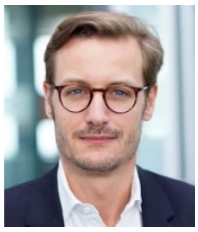
Richard Chudzynski
Data Privacy and Protection Legal Leader
PwC Legal Middle East
+971 56 417 6591
richard.chudzynski@pwc.com

Let's talk

For a deeper discussion of how this impacts your business, please contact us.

Pat Moran
Partner
PwC Ireland
+353 (0) 8638 03738
pat.moran@pwc.com

Grant Waterfall
Partner and Cyber Security & Privacy Leader
PwC Germany
+49 69 9585 5377
grant.w.waterfall@pwc.com



Manuel Seiferth
Partner, Cyber Security & Privacy Strategy, Risk and Compliance
PwC Germany
+49 160 536-3800
manuel.seiferth@pwc.com

Philipp Rosenauer
Partner
PwC Legal, Switzerland
+41 58 792 18 56
philipp.rosenauer@pwc.com

Maressa Juricic
Privacy and Cybersecurity Partner
PwC Brasil
maressa.juricic@br.pwc.com

Bram van Tiel
Partner, Cybersecurity and privacy
PwC Netherlands
+31 (0)88 792 53 88
bram.van.tiel@pwc.com

Csilla Dékány
Attorney-at-law
PwC Hungary
csilla.dekany@pwc.com

Andrea Lensi Orlandi Cardini
New Law Leader
IP, IT, Cybersecurity and Data Protection
PwC TLS Avvocati e Commercialisti
+39 3479162891
andrea.lensi@pwc.com

Chiara Giannella
New Law Director
IP, IT, Cybersecurity and Data Protection
PwC TLS Avvocati e Commercialisti
+39 346 507 3583
chiara.giannella@pwc.com

www.pwc.com

www.tiangandpartners.com

pwc

Tiang & Partners
程偉賓律師事務所