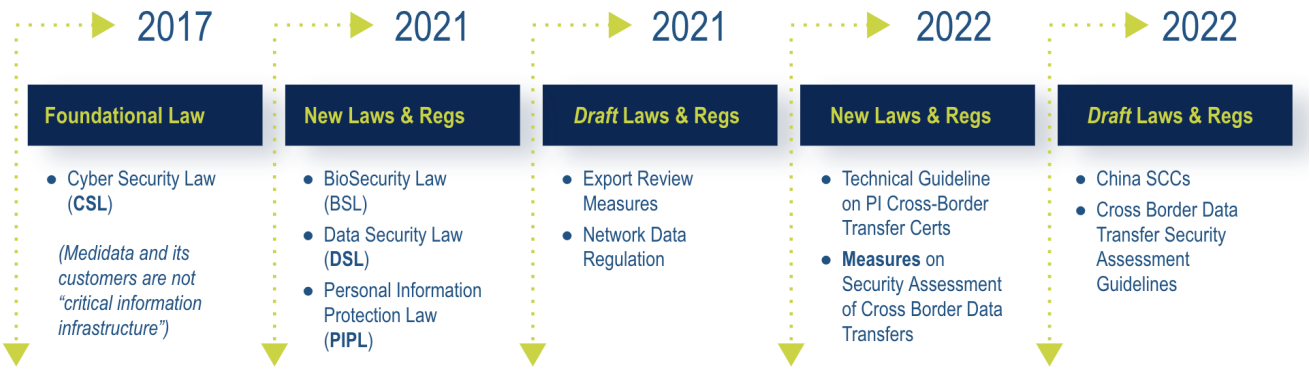
China's New Data Protection Laws and Regulations: Information for Medidata's clients

Medidata's Unified Protection Strategy groups (Privacy, Quality and Security) have been closely assessing how China's new data protection laws, regulations and guidelines apply to your use of our clinical trial technology.

We are pleased to provide you with this Information Sheet focused on key topics relevant to your use of the Medidata Clinical Cloud. Our guidance is informed by discussions with many of our leading sponsors and partners and our participation in life sciences industry groups. We welcome discussions with your subject matter experts as China's dynamic data protection landscape continues to develop.

While China's data protection laws, regulations and guidelines continue to develop…



… these key topics are applicable to the Medidata Clinical Cloud:

- Data localization: Under current laws and regulations, there is no localization requirement relevant to your data in the Medidata Clinical Cloud. Data localization is not required as neither Medidata nor our clients have been deemed to be CIIOs; key-coded clinical trial data has not been designated as Important Data. In addition, the CAC has not issued guidance on data volume thresholds applicable to data localization.

- Cross-border data transfers: Our clients as "data handlers" need to undertake self-assessments in order to ascertain whether their transfers require use of China's Standard Contractual Clauses, or instead a Security Assessment application (See PIPL Sec. 38). This choice will turn on determining the total volume of personal information for which each client is the data handler (See Assessment Measures on Cross-Border Transfer of Data ("Measures")). Under the Measures, it is important to note that neither Medidata nor its clients are considered to be CIIOs, nor is any of the personal information involved deemed to be Important Data.

- Security Assessment under the Measures: To assist our clients' self-assessments and any Security Assessment applications, Medidata has prepared "Security Assessment Questionnaire Responses" in its capacity as an overseas recipient, based on the CAC's template Risk Assessment Report for Cross-Border Data Transfer. Please find these Responses, and other helpful materials such as our "SCC Transfer Impact Whitepaper" (together "Medidata's Security Assessment Materials") on Medidata.com/Trust.

- Separate consent for cross-border data transfers: Data handlers must obtain a "separate consent" to transfer personal information out of China. We advise our clients to obtain this from study participants as part of their existing research consent workflow. Both Medidata and our clients are independent data handlers for the user profile information of Authorized Users (our clients' site investigators and China-based employees). Medidata will work with our clients to help ensure these separate consents are obtained.

- Rights for China individuals: Similar to the EU's GDPR, China's PIPL provides specified and expanded rights to personal information, such as access, correction, deletion, restriction of processing and portability. While guidance on the applicability of these rights to clinical trials that are conducted under other applicable regulations such as ICH GCP is outstanding, Medidata is ready to assist its clients to comply in full.

- Privacy by Design: Unlike the EU's GDPR, which specifically requires Privacy by Design, PIPL does not explicitly contain this requirement. At the same time, Medidata's services are designed from the outset based on universal data protection principles, e.g., restricting personal information processing to only what is necessary for our clients' processing purposes.

- Security: Medidata's data protection framework and security standards set the standard in the life sciences industry, and are confirmed by rigorous third-party attestations and certifications. Among other measures, the Medidata Clinical Cloud provides encryption in transit (with Transport Layer Security) and encryption at rest for our clients' personal information (with AES-256 encryption).

Answers to some frequently-asked questions

Why use Medidata's Security Assessment Materials, instead of using your own vendor-facing questionnaires?

We understand the criticality of our clients' need to self-assess and to meet the security assessment requirements (if applicable) under the Measures and the efforts many have made related to the Risk Assessment Report for Cross-Border Data Transfer, e.g., drafting their own vendor-facing questionnaires. Medidata's Security Assessment Materials cover all topics assessed by the Measures relevant to Medidata's services. Importantly, our Security Assessment Materials provide ready-to-use responses that provide consistency, transparency and efficiency to both our clients and to regulators.

Who should I contact if my company's SME would like to have a more in-depth discussion on data protection in China with Medidata?

We very much welcome discussions on the important topics covered in this Information Sheet. If your company's SMEs would like to have an in-depth discussion with us, please contact us at dataprivacy@medidata.com. You can also contact your account manager.

Where can I find Medidata's data governance program, certifications, and learn more about Medidata's data protection program?

Please visit Medidata.com/Trust for links to our materials relevant to demonstrating your compliance with China's data protection requirements, such as our Information Security whitepapers, our SCC Transfer Impact Whitepaper (prepared to assist our clients with their EU-required TIAs) and our industry-leading SOC2+ attestation and ISO certifications. You can also contact your account manager.

What is Medidata's Unified Protection Strategy?

Medidata's Unified Protection Strategy encompasses our secure, stable, and scalable cloud platform, robust data governance processes, and an inspection-ready quality management system – all critical enablers to your successful clinical trial execution. Our Information Security, Privacy, and Quality Management teams work in unison to safeguard your data and provide solutions that ensure your regulatory compliance.

Key Concepts in China's New Data Protection Laws

CIIO: refers to "critical information infrastructure operator". Data localization is required for entities that are deemed to be CIIOs according to CSL and Section 40 of the PIPL.

Important Data: Introduced in CSL, Important Data currently includes data related to national security, the lifeline of the national economy, and major public interests. Data deemed Important Data requires special protection, e.g., it would likely trigger data localization as well as the CAC security assessment for cross-border data transfers.

CAC: established in May 2011, the Cyberspace Administration of China ("CAC") oversees China's cyberspace security and internet content regulation and enforcement.

Our roles – Data handlers and Entrusted Parties: For our clients' clinical research data, Medidata is the "entrusted party" or "overseas recipient" under PIPL; this is equivalent to the data processor role under the EU's GDPR. Our clients are the "data handler" of this data under PIPL, which is equivalent to the "data controller" role under the GDPR. As the entrusted party, Medidata processes our clients' personal information solely according to their instructions.

Medidata's Life Science Industry-leading Security Standards

Medidata is proud of its long history of successful independent certification and attestation for security, quality, confidentiality, availability, processing integrity, and privacy controls. Visit our Trust & Transparency Center at www.medidata.com/trust to review our reports and certifications in detail.

SOC 2 Type 2: Medidata publishes a Service Organization Controls 2 (SOC 2) report conducted in accordance with SSAE 16 and the ISAE 3402 professional standards. The SOC 2 report audit attests that Medidata control objectives are appropriately designed and operating effectively, including in compliance with the AICPA **Privacy Trust Services Criteria,** an *industry first*.

Ver. Dec. 2022