VIEW POINT

NAVIGATING NEW BOUNDARIES: LIFE SCIENCES IN THE AGE OF DSL AND PIPL

Abstract

As China continues to shape its digital landscape through the implementation of stringent regulations like the Data Security Law (DSL) and the Personal Information Protection Law (PIPL), organizations operating in or engaging with the Chinese market face unprecedented challenges and opportunities. This PoV delves into the nuances of these regulations, examining their implications for level service companies that navigate the complexities of compliance and data management. By analyzing the core tenets of DSL and PIPL, our research identifies the key operational adjustments required for firms to maintain competitiveness while ensuring regulatory adherence. Furthermore, we explore the potential impacts on data governance, customer trust, and service delivery models, offering actionable insights for organizations striving to adapt to this evolving regulatory environment. The findings highlight not only the pivotal importance of robust compliance strategies but also the potential for leveraging new regulations as a catalyst for innovation in service offerings. With these insights, businesses can better align their operations with the regulatory expectations, ultimately fostering sustainable growth in a dynamic market characterized by regulatory evolution and heightened consumer awareness.

Infosys®
Navigate your next

Introduction to China's PIPL and DSL Law

The rapid evolution of data protection and cybersecurity regulations in China, notably the Data Security Law (DSL) and the Personal Information Protection Law (PIPL), presents significant challenges and strategic implications for life sciences companies operating within or interacting with the Chinese market. These regulations impose rigorous compliance requirements concerning data management, privacy protection, and cybersecurity protocols that fundamentally affect how life sciences companies conduct research, manage clinical data, and safeguard sensitive patient information. As the sector increasingly relies on data-driven decisions, the complexities of navigating these regulatory frameworks threaten to disrupt established business models and impede innovative advancements in research and development.

Consequently, life sciences companies must grapple with the dual challenge of ensuring compliance while simultaneously leveraging the regulatory landscape to enhance their service offerings, optimize operational efficiencies, and maintain competitive advantage. This PoV seeks to analyze these regulatory impacts, identify the critical issues faced by life sciences firms, and propose strategic frameworks that will enable them to adapt effectively to these new regulations while fostering growth and innovation in their service delivery.

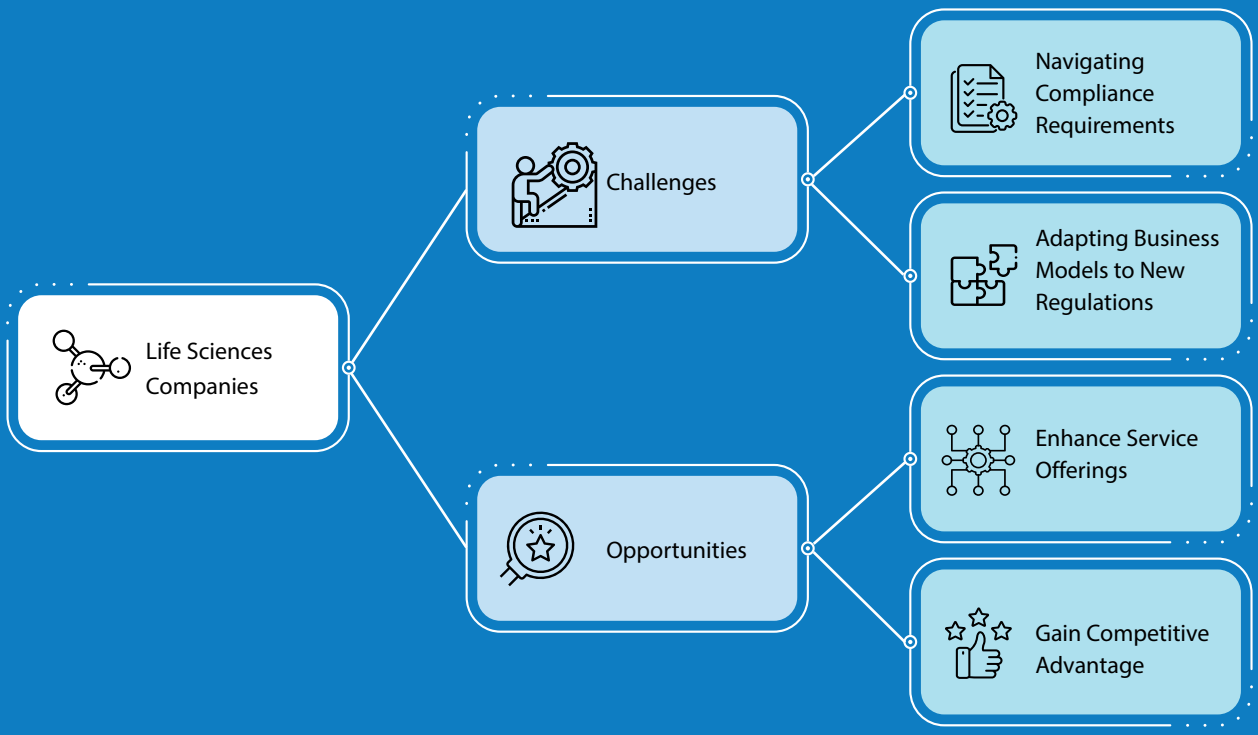
China's Data Security Law (DSL) and Personal Information Protection Law (PIPL) are laws that govern data processing and cybersecurity in China.

Data Security Law (DSL)

- Focus on data security from a national security perspective.
- Requires businesses to categorize data by importance.
- Restricts cross-border data transfers.
- Applies to all data processing activities (online and offline).
- **Effective Date**: September 1, 2021.

Personal Information Protection Law (PIPL)

- Protects the personal information of Chinese citizens (like the EU's GDPR).
- **Rights of Data Subjects**:
  - Right to access, correct, and delete their data.
- **Obligations of Organizations**
  - Transparency in data processing.
  - Obtaining consent where necessary.
  - Adopting security measures for data protection.
- **Effective Date**: November 1, 2021.



Navigating Compliance Requirements

Compliance with the Data Security Law (DSL) and the Personal Information Protection Law (PIPL) can be complex. Companies must implement measures to protect personal data and ensure their data practices meet stringent standards.

Key Considerations:

- Continuous changes in regulations necessitate regular updates to compliance strategies.
- Heavy penalties for non-compliance necessitate robust compliance frameworks and monitoring systems.

Adapting Business Models to New Regulations

Existing business models may need re-evaluation. For example, how data is collected, processed, and shared in R&D processes must align with new legal frameworks.

Key Considerations:

- Strategic partnerships and collaborations may be required for international compliance.
- Companies may need to pivot towards more sustainable and ethically responsible practices which could require significant investment.

Enhance Service Offerings

By ensuring compliance with PIPL and DSL, companies can build trust with customers and stakeholders, facilitating the expansion of their service offerings.

Key Strategies:

- Develop enhanced privacy programs that differentiate them in the marketplace.
- Utilize state-of-the-art technologies such as AI and data analytics in compliance solutions to add value to service offerings.

Gain Competitive Advantage

Companies that successfully navigate these regulations can position themselves as leaders within the Life Sciences sector, leveraging compliance as a unique selling proposition.

Key Strategies:

- Foster innovation by integrating compliance as a hallmark of company culture, streamlining operations, and improving data integrity and security.
- Be proactive rather than reactive in addressing regulatory changes, which could lead to long-term sustainability.

Key Requirements for PIPL and DSL Compliance

The legal implications for life science companies span across all operational domains, especially in data governance, IT security, and compliance management. PIPL mandates the protection of personal data, emphasizing the need to safeguard sensitive data such as medical records, genetic data, and patient information. Some key requirements for compliance with China's Data Security Law (DSL) and Personal Information Protection Law (PIPL) include:

Data categorization
The DSL establishes a hierarchical system for data based on its importance to national security, public interest, and individual rights.

Data localization
The PIPL imposes restrictions on cross-border data transfers and mandates data localization for certain types of sensitive personal information. Organizations may face challenges in establishing or modifying infrastructure to comply with these requirements.

Cross-border data transfer
Organizations conducting cross-border data transfers must meet stringent requirements under the PIPL, including conducting security assessments and obtaining approval from regulatory authorities. Navigating these requirements while maintaining business operations can be challenging, particularly for multinational companies.

Data Collection and Consent
The PIPL requires obtaining consent to process personal data, and separate consent is required for certain significant processes. Consent is only valid if it is knowingly and explicitly granted, with full information of the extent of personal information processing.

Breach notification
When personal information is lost, tampered with, or leaked, personal information processors must immediately take remedial actions and notify individuals and personal information protection authorities.

Disclosure of personal information
The PIPL introduces the concept of "sensitive personal information," which can easily lead to personal dignity infringement or endanger personal or property security.

Accountability and governance
The PIPL imposes accountability requirements on PI (personal information) handlers, including developing an internal management system and operating procedures.

Now we will focus on the risk patterns and scenarios related to PIPL and DSL Compliance

Risk Pattern and Scenarios Related to PIPL and DSL Compliance

Non-compliance with PIPL, and DSL exposes Life Sciences companies to various risks, including financial penalties, reputational damage, and operational disruptions. Common risks scenario include:

- Inadequate Consent Management on Data Use or Transfer Abroad
- Insufficient Data Security Measures
- Failure to Implement Data Subjects Rights
- Cross-boarder Data Transfer
- Third-party Risk Management
- Lack of employees Training Awareness

PIPL Fines for Non-Compliance

The PIPL hands down severe fines for businesses that do not comply with its regulations. First offenses often result in a warning and a strict order for a business to change its policies and align with the PIPL's requirements.

After receiving a warning, if a business still does not comply with the PIPL, the personal information protection authorities will charge businesses fines of varying degrees.

A business can face a fine of up to **1 million yuan** (**$150,000**) for minor violations; in some cases, specific individuals in charge will be fined.

The PIPL charges individuals responsible (often the data protection officer) are typically subject to fines between **10,000** to **100,000 yuan** (**$1,500-$15,000**) for minor violations. An example of DSL and PIPL law violation:

Didi Case

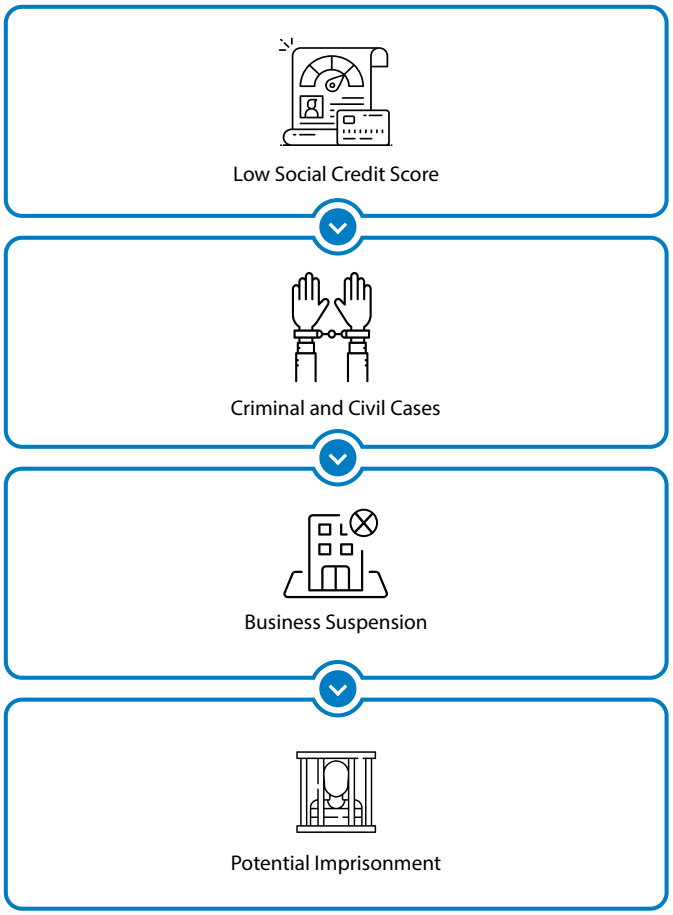
CAC, China's national enforcement agency, held that rideshare platform Didi had committed serious violations of PIPL, DSL, and CSL. Didi was found to have engaged in illegal collection of excessive data from users' mobile phones, including call logs, contact details, location data, photo albums, and apps.

The Cyberspace Administration of China (CAC) fined Didi a total of 8 billion yuan (approximately **$1.2 billion**) for violating the PIPL, CSL (Cybersecurity Law), and DSL.

The CAC found that Didi had collected excessive amounts of data from users, including contact information, location data, and photos.

The fine amounted to more than **4%** of Didi's total revenue for the previous year. A total of 16 violations of the law were identified.

Other Consequences of Non-compliance with PIPL



As we have figured out the risk patterns and scenarios related to PIPL and DSL compliance and discussed over the consequences if any company violates these laws, now, we will discuss further how this PIPL and DSL law will impact the life science industry, and their business processes and systems. As we have to more closely focus on making the business processes more compliant with China's laws.

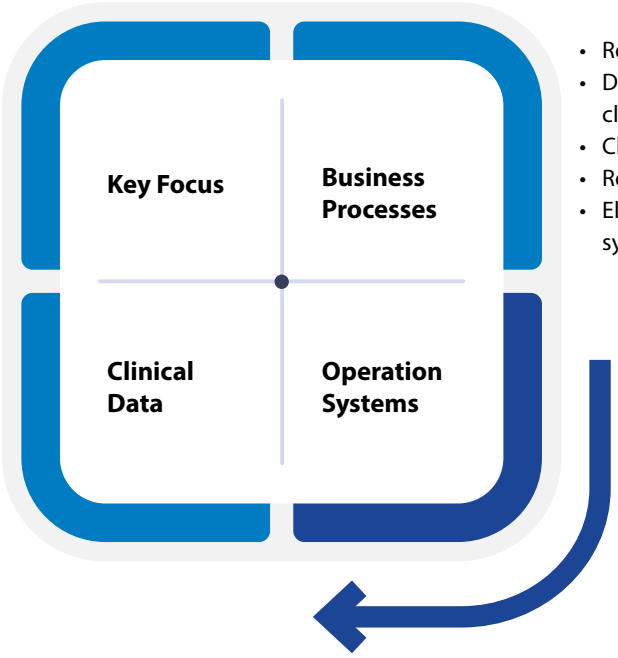
Impact on Life Science Industry

A range of Business Processes within life sciences are directly impacted by data protection requirements. The PIPL extends to all aspects of life science R&D, including clinical trials, data analysis, and patient recruitment. It requires companies to adhere to stringent data protection standards when handling patient health information, genetic data, and other sensitive information.

The law introduces new regulations governing the collection, storage, and use of data in clinical trials, impacting participant consent, data security, and data sharing practices.

- Cross border data transfer
- Third party integration
- Regulatory process
- Data entities that resides and are transfered between business process and application

- Laboratory data
- IP Sample data
- Inform consent form
- Subject visit progress
- Patient data, screening logs
- Employee data, customer data, salary information
- Patient demographics, medical records, financial data



- Research & development
- Data collection and processing in clinical trials
- Clinical data management
- Regulotory compliance
- Electronic trial management filing system

Laboratory Information Management Systems (LIMS)	• Patient identifiers linked to samples (e.g., medical record numbers) • Results of laboratory tests • Health conditions related to the samples being processed
Clinical Trial Management Systems (CTMS)	• Participant names • Contact information • Demographic information (age, sex, ethnicity) • Health data and medical history related to trial participation • Consent documents
Electronic Health Record (EHR) Systems	• Patient names • Dates of birth • Medical history • Treatment information • Medications • Allergies • Contact information
Customer Relationship Management (CRM) Systems	• Contact information of healthcare providers • Patient information for marketing, education, or outreach efforts • Feedback and communications linked to individual patients
Supply Chain Management Systems (SCM)	• Supplier and vendor details (potentially including contact information) • Shipment tracking information linked to recipient individuals (e.g., patient addresses for home delivery of medications)
Pharmacovigilance Systems	• Patient names and demographics • Reports of adverse drug reactions • Health histories relevant to incidents reported
Regulatory Compliance Management Systems	• Employee information (e.g., compliance officers, quality assurance personnel) • Patient data related to regulatory submissions, if applicable
Data Analytics and Decision Support Systems	• Aggregated patient data used for research studies or statistical analysis • Demographic information utilized in analysis of treatment outcomes

Business Process and its Challenges

Research & Development

Challenges:

- **Data Minimization:** Determining necessary data while ensuring completeness and accuracy can be challenging.
- **Transparency and Consent:** Obtaining informed consent from research participants, particularly in clinical trials, requires clear communication about the research process and data usage.
- **Cross-Border Data Transfer:** Transferring research data or collaborating with international partners can be complex due to restrictions and requirements under the PIPL.

Data Collection and Processing in Clinical Trials

Challenges:

- **Enhanced Consent Requirements:** Informed consent must be obtained for specific data collection, clearly outlining the purpose, scope, and duration of data use.
- **Data Minimization:** Only necessary data relevant to the trial objectives should be collected, minimizing the amount of personal information processed.
- **Data Security Measures:** Stronger security measures are required to protect sensitive data, including encryption, access controls, and data breach notification procedures.

Enabling Compliant Data Management

Challenges:

- **Data Anonymization:** Use data anonymization techniques to remove personally identifiable information from clinical trial datasets.
- **Access Control:** Implement access controls to restrict access to clinical trial data based on user roles and permissions.
- **Data Governance:** Establish strong data governance policies and procedures to ensure data quality, integrity, and compliance.

Evolving Regulatory Landscape

Challenges:

- **Guidance Updates:** Regulatory authorities will continue to issue guidance and clarification on DSL and PIPL interpretation.
- **Enforcement Actions:** Expect increased enforcement actions against companies that fail to comply with data privacy regulations.
- **New Regulations:** China may introduce new regulations or amendments to existing laws to further strengthen data protection.

Third-Party Compliance

Challenges:

- **Data Storage and Processing:** Organizations may rely on third-party service providers for various data processing activities, including data storage and processing.
- **Data Oversight and Accountability:** Ensuring that these third parties comply with the requirements of the PIPL and adequately protect personal data presents additional challenges in terms of oversight and accountability.

Evolving Electronic Trial Master File (eTMF)

Challenges:

- **Data Security:** Obtaining specific consent before processing sensitive personal information and/or important data, which can be done through inclusion in current consenting workflows.
- **Data Assessment:** Completing a personal information protection impact assessment, as necessary.

Operating Systems and Their Implications and Compliance Strategies

LIMS

Implications

- **Data Collection Practices:** LIMS systems must ensure that data collection practices are compliant with PIPL requirements, including obtaining informed consent and minimizing data collection. A laboratory information management system (LIMS) stores a variety of data, including sample information, test results, and quality control data.
- **Data Security Measures:** LIMS systems contain quality control data instrument readings and quality control data. It must be implemented with robust data security measures to protect personal information from unauthorized access, disclosure, alteration, or destruction.
- **Cross-Border Data Transfers:** Organizations using LIMS systems must be aware of the restrictions on cross-border data transfers and ensure compliance with PIPL requirements.

Compliance Strategies

- **Data Inventory:** Conduct a comprehensive inventory of all personal information processed by the LIMS system.
- **Data Security Assessment:** Evaluate the current security measures in place and identify any gaps in compliance with PIPL requirements.
- **Data Retention Policies:** Develop and implement clear data retention policies that comply with PIPL requirements and ensure the deletion or anonymization of data that is no longer necessary.
- **Data Transfer Agreements:** Establish data transfer agreements with third-party vendors and recipients of data outside China, ensuring compliance with PIPL requirements.

Clinical Trial Management System

Implications

- **Compliance:** CTMS must adhere to PIPL requirements, as CTMS stores a variety of data, including patient information, study documents, and vendor information.
- **Operational Changes:** Tracks anonymized subject records for high-level enrollment tracking and data usage in site payments and visit report authoring. Impacts include modifications in data collection, consent processes, and data storage.
- **Data Handling Practices:** Organizations must ensure data collection and storage practices align with new regulations, necessitating updates to existing CTMS protocols.
- **Informed Consent Management:** The need for robust systems to manage patient consent forms is critical under the PIPL, which mandates explicit consent for data usage.

Compliance Strategies

- **Encryption:** Encrypt sensitive data at rest and in transit.
- **Access Control:** Implement role-based access control to limit data visibility.
- **Data Masking:** Mask or redact sensitive information during analysis.
- **Auditing:** Regularly audit system access and data processing.

ERP Systems

Implications

- **Employee Data:** ERP systems often store sensitive information about employees, including salaries, contact details, and performance data. PIPL requires organizations to obtain clear consent for using this data.
- **Customer Data:** ERP systems may also contain customer data, such as purchase history, contact details, and preferences. This data is subject to the PIPL's requirements for consent, transparency, and data security.

Compliance Strategies

- **Review and Update:** Review and update your ERP system's configuration and settings to align with PIPL requirements.
- **Assess and Improve:** Assess your current data security measures and implement any necessary improvements.
- **Implement Data Protection Controls:** Consider implementing data protection controls, such as encryption and access controls, to enhance data security.
- **Data Mapping:** Conduct a thorough data mapping exercise to identify all personal data processed by your ERP system.

CRM Systems

Implications

- **Patient Demographics:** Name, date of birth, address, contact information, and other identifying information are considered sensitive and require stringent protection.
- **Medical Records:** Diagnosis, treatment history, medications, test results, and other sensitive medical information must be handled with the highest level of confidentiality.
- **Financial Data:** Insurance details, billing information, and payment records are protected under the PIPL and require secure handling.

Compliance Strategies

- **Data Privacy Assessment:** Conduct a comprehensive data privacy assessment to identify and address potential risks related to personal information processing.
- **Policy and Procedure Development:** Develop and implement clear policies and procedures for handling personal information, including data collection, storage, and transfer.
- **Employee Training:** Provide comprehensive training for all employees involved in data handling, emphasizing data privacy principles and best practices.
- **Data Minimization:** Streamline data collection practices to minimize the amount of personal information collected.
- **Consent Management:** Implement a robust consent management system to obtain informed consent from individuals before processing their data.
- **Data Security:** Invest in advanced security measures to protect personal information from unauthorized access, use, or disclosure.
- **Data Localization:** Evaluate the feasibility of storing sensitive personal information within China's territory to comply with the PIPL's localization requirements.

Supply Chain Management

Implications

- **Data Privacy and Protection:** Companies must implement robust data handling protocols and ensure that operational systems are equipped to manage PI responsibly, including obtaining explicit consent for data use.
- **Increased Transparency and Reporting:** Implement systems capable of generating compliance reports and conduct regular audits to ensure adherence to the laws, which can lead to increased operational complexity and resource allocation.
- **Data Localization Requirements:** Organizations must reassess their SCM architecture to ensure data locality, which may involve significant investment in local infrastructure and alignment of global data strategies.

Compliance Strategies

- **Conduct Thorough Compliance Audits:** Regular audits of operational systems can help identify potential gaps in compliance with the DSL and PIPL. This proactive approach enables organizations to address vulnerabilities before they lead to regulatory infractions.
- **Develop a Comprehensive Data Governance Framework:** Establish clear policies around data handling, including data classification, consent management, and access controls. Training employees in these policies ensures that all team members understand their responsibilities regarding data privacy and security.
- **Invest in Localized Infrastructure**

Pharmacovigilance Systems

Implications

- **Data Security Requirements:** Pharmacovigilance systems must implement data encryption, secure transmission protocols, and regular security audits to ensure the confidentiality, integrity, and availability of personal health data.
- **Data Localization:** Pharmacovigilance systems must store sensitive personal data within China or ensure compliance with China's data localization regulations.
- **Data Cross-Border Transfer:** Pharmacovigilance systems must obtain approval before transferring high-risk personal data from China to foreign countries.
- **Data Anonymization:** Pharmacovigilance systems must anonymize or pseudonymize personal health data to minimize the risk of personal information disclosure.

Compliance Strategies

- **Conduct a Data Mapping Exercise:** Identify all personal health data collected, stored, or used within the pharmacovigilance system, including data types, data sources, and data usage purposes.
- **Implement Robust Security Measures:** Implement data encryption, secure data transmission protocols, and regular security audits to protect personal health data.
- **Develop a Data Governance Framework:** Establish a clear data governance framework to ensure data collection, use, and disclosure comply with the DSL and PIPL regulations.
- **Develop a Data Localization Plan:** Ensure all sensitive personal data are stored within China or comply with the data localization regulations.
- **Develop a Cross-Border Transfer Plan:** Obtain necessary approval before transferring high-risk personal data from China to foreign countries.

Regulatory Compliance Management Systems

Implications

- **Increased Compliance Complexity:** The dual requirements of DSL and PIPL introduce new layers of compliance for healthcare entities, necessitating sophisticated RCMS capabilities that address both data security and privacy in parallel.
- **Data Governance Enhancements:** RCMS must include comprehensive data governance frameworks, adapting to maintain compliance with classification requirements, data handling protocols, and consent management.
- **Risk Management:** Enhanced risk assessment procedures must encompass not just operational risks, but also data security and privacy risks specific to personal health information (PHI).
- **Stakeholder Training and Awareness:** Successful compliance will require a robust training framework within RCMS, ensuring that all stakeholders understand their responsibilities under the new laws.
- **Operational Inefficiencies:** Failure to adapt compliance and regulatory processes could result in operational inefficiencies, affecting the organization's ability to deliver timely healthcare services.

Compliance Strategies

- **Conduct Comprehensive Data Mapping:** Identify and classify all patient and health service data types. Distinguish between sensitive and non-sensitive data according to DSL classification guidelines.
- **Integrate Consent Management Systems:** Develop systems for obtaining and documenting explicit consent. Provide transparent options for individuals regarding the use of personal information.
- **Build a Robust Data Governance Framework:** Establish policies and procedures for data management, including access controls, data retention, data breach responses, and third-party compliance standards.
- **Emphasize Predictive Risk Assessment:** Incorporate predictive analytics into risk assessment processes to identify potential compliance failures before they occur, focusing on both internal practices and external regulatory changes.
- **Implement Technology-Driven Solutions:** Leverage technology such as automated compliance monitoring tools, data encryption, and anonymization techniques to enhance data security while simplifying compliance workflows.
- **Establish a Training and Awareness Program:** Regularly train staff in data protection and compliance with regulations. Foster a culture of security and privacy organization wide.
- **Regular Auditing and Reporting:** Schedule regular audits of compliance activities related to the DSL and PIPL and establish clear internal and external reporting channels for data breaches or compliance failures.
- **Develop Incident Response Plans:** Create and maintain a data breach response plan that aligns with the incident reporting requirements of both the DSL and PIPL, ensuring prompt action in the event of a data breach.

Data Analytics and Decision Support Systems

Implications

- **Data Governance and Classification:** Healthcare organizations must thoroughly understand and implement data classification processes to manage the entirety of their datasets. This includes distinguishing between general health data and sensitive personal information.
- **Enhanced Privacy Protections:** Systems used for analytics must integrate strong data privacy measures, ensuring that personal information is processed and anonymized according to PIPL requirements.
- **Limited Data Accessibility:** With regulations restricting data transfers and requiring specific security assessments, organizations might encounter challenges regarding data accessibility for analytic purposes.
- **Increased Compliance Burden:** The need for continuous monitoring and auditing to ensure compliance with both DSL and PIPL may increase operational complexities and resource allocation toward compliance activities.
- **Ethical Considerations:** The ethical implications of data analytics in healthcare must be reassessed, particularly regarding patient consent and data use.

Compliance Strategies

- **Implement Data Governance Frameworks:** Establish clear data governance policies that define roles and responsibilities related to data collection, processing, and analytics. Classify data according to the DSL standards, ensuring that sensitive and personal data are identified and managed appropriately.
- **Anonymization and Pseudonymization:** Utilize anonymization or pseudonymization to protect personal data used in analytics. This minimizes the risk of identity exposure while still providing valuable insights.
- **Robust Consent Management:** Develop processes for obtaining, managing, and documenting patient consent in relation to data collection and analytics. This ensures compliance with PIPL's strict consent requirements. Consider implementing opt-in mechanisms where patients may choose how their data is used in analytics.
- **Regular Risk Assessments:** Conduct ongoing risk assessments related to data analytics practices to identify potential compliance gaps and mitigate risks associated with data security and privacy.
- **Monitor Data Access and Usage:** Set up comprehensive monitoring systems to track data access and usage patterns, ensuring that analytics are conducted solely for permitted and legitimate purposes as outlined in patient consent.

Impact of PIPL and DSL on Life Sciences and Its AI Applications

Refer to large-scale AI models that are trained and deployed in specific geographic locations or within organizations. They are tailored to understand and generate human-like text based on the context provided, while being sensitive to the local language, culture, regulations, and data requirements.

For the life sciences industry in China, a local LLM could be designed to understand and process scientific literature, clinical protocols, and patient data while adhering to the regulatory frameworks imposed by the Personal Information Protection Law (PIPL) and the Data Security Law (DSL).

Incorporating Responsive AI in LLMs

Responsive AI refers to the AI's capability to react and adapt based on user interactions, ethical constraints, and regulatory requirements. To dovetail this concept with LLMs in the context of PIPL and DSL, particularly in the life sciences sector, consider the following aspects:

Strategies for Incorporating Responsive AI

Data Privacy and Compliance Mechanisms

- **Real-time Compliance Checks:** Implement algorithms in the LLM that continuously check the data being utilized against compliance requirements of PIPL and DSL. This may involve identifying personally identifiable information (PII) and ensuring it is handled appropriately.
- **Dynamic Consent Management:** Incorporate modules that can manage and track consent from users dynamically, allowing users to revoke access to their data at any time. This helps ensure that the legal aspects of data handling are respected.

Adaptive Learning Models

- **Continuous Training:** Design LLMs that can adapt and learn from new data as regulations evolve. This might include regularly updating the model with new guidelines, best practices, or feedback from compliance audits.
- **Customization Based on Use Cases:** Tailor the LLM's responses and capabilities based on specific applications like clinical data analysis, drug discovery, or patient engagement while keeping responsiveness to regulatory guidelines.

Ethical and Responsible AI Practices

- **Bias Detection and Mitigation:** Implement mechanisms within the LLM to identify and mitigate any biases that may arise in the training data or model outputs. This ensures that the AI-generated insights are ethical and in line with fair treatment practices outlined by PIPL.
- **Transparency and Explainability:** Enable the LLM to provide explanations for its outputs or recommendations, thus fostering trust and understanding among users while adhering to the principles of transparency outlined in data protection laws.

Advanced Security Measures

- **Data Anonymization and Encryption:** Integrate responsive AI capabilities that automatically anonymize sensitive data before it is processed by the LLM. This aligns with DSL requirements regarding sensitive data processing.
- **Access Control Protocols:** Develop fine-grained access controls that adapt based on user roles and data sensitivity. This could involve using AI to monitor and adjust access rights based on the compliance landscape.

Feedback Loops

- **User Feedback Integration:** Create responsive channels for users to provide feedback on AI's outputs. The LLM can learn from real-world usage patterns, allowing it to provide more relevant and compliant responses over time.
- **Incident Reporting:** Incorporate features that allow users to report any compliance or ethical concerns regarding AI interactions, enabling timely adjustments to the model or its application.

Regulatory Monitoring and Updates

- **Automated Updates on Regulations:** Build a responsive mechanism that regularly reviews changes in PIPL and DSL and integrates those changes into the LLM's operating framework.
- **Partnerships with Regulatory Experts:** Collaborate with legal experts to ensure that the LLM remains aligned with compliance requirements, utilizing AI to facilitate ongoing regulatory engagement.

Infosys Solution Approach

Leverage the knowledge and experience of the currently managed services team in Global SFA (Sales Force Automation)/local apps solutions to improve quality and risk mitigation.

As the Clinical Trial Management System (CTMS) is a widely used ecosystem in the life sciences industry, we are bringing Veeva Vault as a solution to serve as a platform that can manage clinical trial planning, data collection, and reporting, improving efficiency and compliance in research protocol.

Bringing Veeva best practices and accelerators built through our partnership.

Our thought leadership and experience in executing similar data migrations and rehosting in the data and analytics domain for global clients to improve the performance and reliability of solutions.

- China-based leadership team with offshore development/test resources for a cost-effective solution.
- The solution includes a PMO team based in China for collaboration with workstream leads.
- Global SMEs for Veeva solutions to deliver quality solutions. We are a premier partner for Veeva and have proven expertise in delivering Veeva implementation and testing programs for global pharma clients. Also, we have a strong ecosystem partnership with local product vendors in marketing workstreams and data and analytics solutions.
- Leverage Infosys China's legal and advisory support for global clients to meet PIPL and DSL regulations.
- Train and educate the project teams on the regulations.
- Our solution includes hypercare and transition to the existing managed services organization. We are the managed services partner for global SFA. One-Med and local applications make the transition smoother by embedding support resources during the service transition and hypercare period to ensure that business disruption is minimized in this critical program.

Conclusion

China's PIPL and DSL law represent a new era in data protection for China, making compliance not just a legal obligation but also a strategic necessity for life sciences organizations. Infosys solution approach can build a compliance-oriented culture, and adopted systematic remediations can mitigate the risks and strengthen their data protection law. This solution approach from Infosys enables life science organizations to navigate the complexities of PIPL and DSL compliance, ensuring data privacy, legal alignment, and operational efficiency in the face of stringent regulations.

References

- *https://www.morganlewis.com/pubs/2021/10/impact-of-recent-china-data-protection-laws-on-asian-life-sciences-industry*
- *infosys.com/industries/life-sciences/insights/documents/managing-pipl-risks.pdf*
- *https://signanthealth.com/company/news/signant-health-announces-readiness-to-facilitate-customers-compliance-with-chinas-personal-information-protection-law-pipl-for-clinical-trial-data-collection*
- *https://incountry.com/blog/how-should-life-sciences-companies-implement-chinas-pipl-regulations/*
- *https://www.wilmerhale.com/en/insights/client-alerts/20241011-china-finalizes-the-network-data-security-management-regulations-and-issues-the-first-free-trade-zone-data-export-negative-list*

Authors

Amol Dhawale
Lead Consultant

Deepika Sawant
Consultant

Shikha Sharma
Senior Associate Consultant

For more information, contact askus@infosys.com