VIEW POINT

MANAGING PIPL RISKS FOR THE LIFE SCIENCES INDUSTRY

Abstract

With China's Personal Information Protection Law (PIPL) enforcing stringent guidelines on data privacy, compliance has become a critical challenge for life sciences organizations. Based on our own business practices and understanding of PIPL, we explore the impact of PIPL, the associated risks of non-compliance, and how life sciences companies can leverage structured methodologies and compliance frameworks, such as Enterprise Architecture (EA), to build secure, compliant systems. Through these approaches, supported by Infosys China's compliance services, organizations can mitigate risks and build a robust foundation for data privacy and security.

Infosys®
Navigate your next

Introduction

The rapid digital transformation in life sciences has enabled new avenues for data-driven insights, personalized medicine, and efficient healthcare delivery. However, this shift has also introduced challenges, particularly in data privacy, as organizations collect vast amounts of sensitive personal data. The introduction of China's Personal Information Protection Law (PIPL) mandates stricter data privacy regulations, with the potential for severe penalties or even interruption of business operations if organizations fail to comply.

For life sciences companies, which often handle highly sensitive health and genetic data, PIPL compliance is essential—not just to avoid legal consequences, but also to safeguard public trust and uphold ethical standards.

Essential Awareness of China's PIPL: An Overview

PIPL provides a comprehensive framework for regulating the processing of personal data within China. The law defines two types of information:

Personal Information

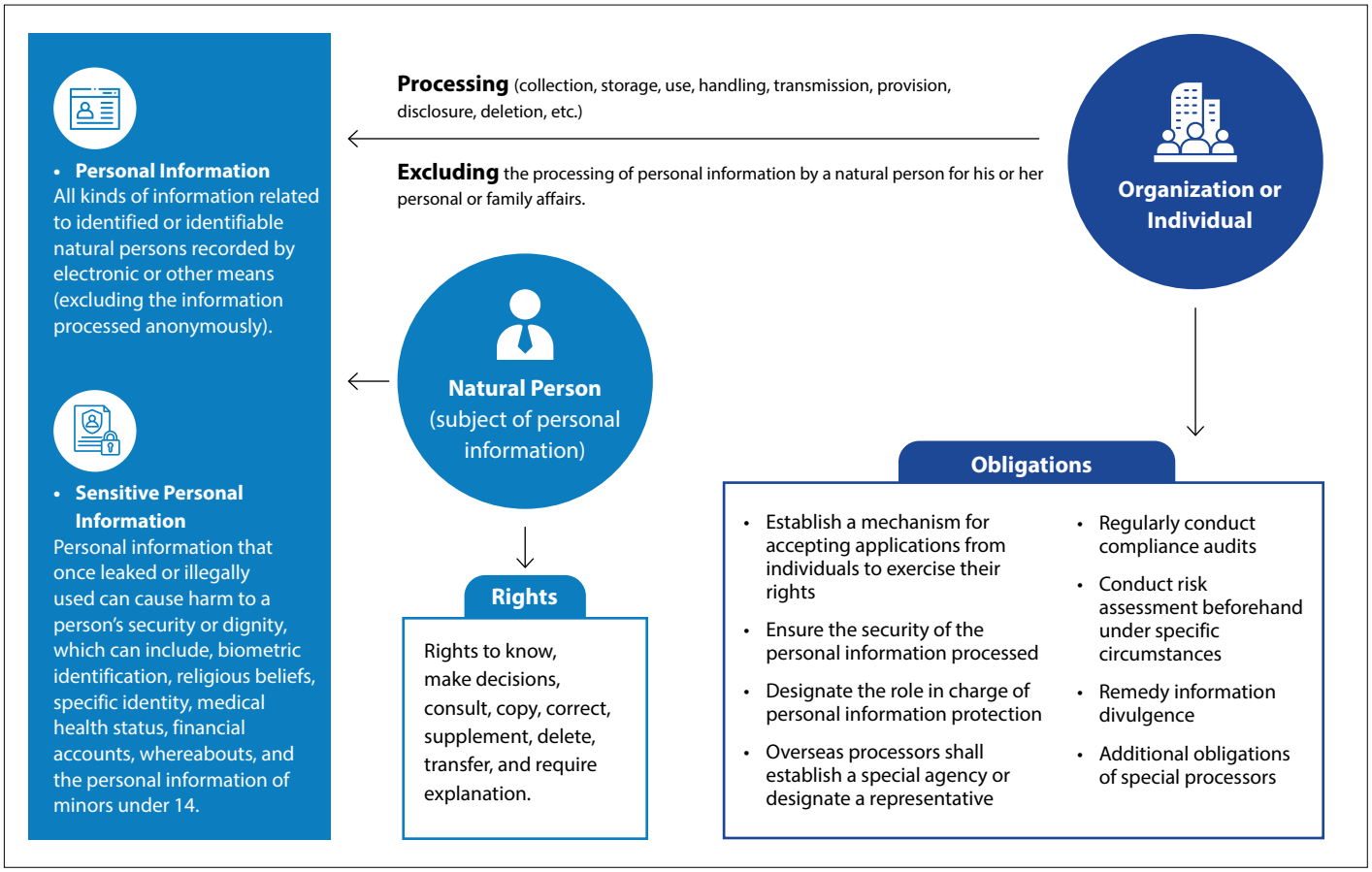
All kinds of information related to identified or identifiable natural persons, recorded by electronic or other means (excluding the information processed anonymously).

Sensitive Personal Information

Personal information, that once leaked or illegally used, may easily lead to the infringement of the personal dignity of a natural person or may endanger his or her personal safety or property. This can include information such as biometrics, religious belief, specific identity, medical health status, financial accounts, the person's whereabouts, as well as the personal information of a minor under the age of 14.

Additionally, PIPL outlines rights for data subjects (such as the right to access, correct, and delete their data) and obligations of organizations (such as ensuring transparency in data processing, obtaining consent where necessary, and adopting security measures to protect personal data). The framework applies not only to companies operating within China but also to foreign companies handling Chinese personal data, making its reach extensive.

Figure 1: An Overview of China's PIPL



Key Requirements of PIPL Compliance

PIPL's implications for life sciences companies span across all operational domains, especially in data governance, IT security, and compliance management.

What

PIPL mandates the protection of personal data, emphasizing the need to safeguard sensitive data such as medical records, genetic data, and patient information.

Who

Organizations processing Chinese personal data must comply with PIPL's requirements, even if they operate outside China.

Where

The law applies within the territory of China but also extends to foreign entities that handle Chinese citizens' data.

These areas highlight key requirements of PIPL on enterprise operations.

Data Collection and Consent:
Explicit consent is required from individuals for data collection, along with IT systems to manage this consent.

Security Measures and Breach Notification:
Adoption of technical measures to protect data and report breaches, with a focus on security technologies and incident response.

Training and Enabling:
Understanding the risks, such as money loss, reputation loss, and business interruption. And assigning responsibilities in combination with business positions.

Data Minimization and Purpose Limitation:
Only necessary data should be collected for specific purposes, highlighting the need for data governance.

Data Transfer and Cross-border Restrictions:
Cross-border data transfers require security assessments or certifications, with systems to ensure compliant data flow.

Individual Rights:
Individuals have rights to access, correct, and delete data, requiring supportive processes and systems.

Risk Patterns and Scenarios Related to PIPL Compliance

Non-compliance with PIPL exposes life sciences companies to various risks, including financial penalties, reputational damage, and operational disruptions. Common risk scenarios include:

Inadequate Consent Management on Data Use or Transfer Abroad

- Inadequate consent for clinical trials and research data
- Lack of valid consent for processing patient data for pharmaceutical marketing or market research
- Insufficient consent management for data sharing with healthcare providers and partners
- Non-compliance with consent requirements for genomic and genetic data handling
- Failure to obtain proper consent for personal health data collected by mobile or wearable devices

Insufficient Data Security Measures

- Unauthorized access to personal health data
- Non-compliance with data minimization and purpose limitation principles
- Inadequate third-party data security assessments
- Insufficient measures to anonymize/de-identify data
- Lack of incident response and breach notification
- Vulnerabilities in applications, middleware, third-party cloud services, and infrastructure

Failure to Implement Data Subject Rights

- Challenges in responding to data access requests
- Inability to fulfill data correction requests
- Delays in processing data deletion requests
- Non-compliance with consent withdrawal
- Insufficient transparency in data processing
- Lack of automation or mechanisms for responding and processing

Cross-border Data Transfer

- Risks associated with clinical trials involving international research
- Challenges in ensuring PIPL compliance when sharing clinical data with global partners
- Compliance risks related to data analysis outsourced to overseas service providers
- Potential for non-compliance when using international cloud services
- Risks of non-compliance when exporting genetic data for international research
- Challenges in maintaining PIPL compliance during cross-border data transfers in mergers and acquisitions

Third-party Risk Management

- Inadequate data processing agreements and oversights with third parties
- Data transfers to third-party in cross-border research
- Inadequate security monitoring of cloud services
- Data sharing with marketing partners without consent
- Failure to implement necessary data anonymization
- Outsourcing data processing to third parties without assessments

Lack of Employee Training and Awareness

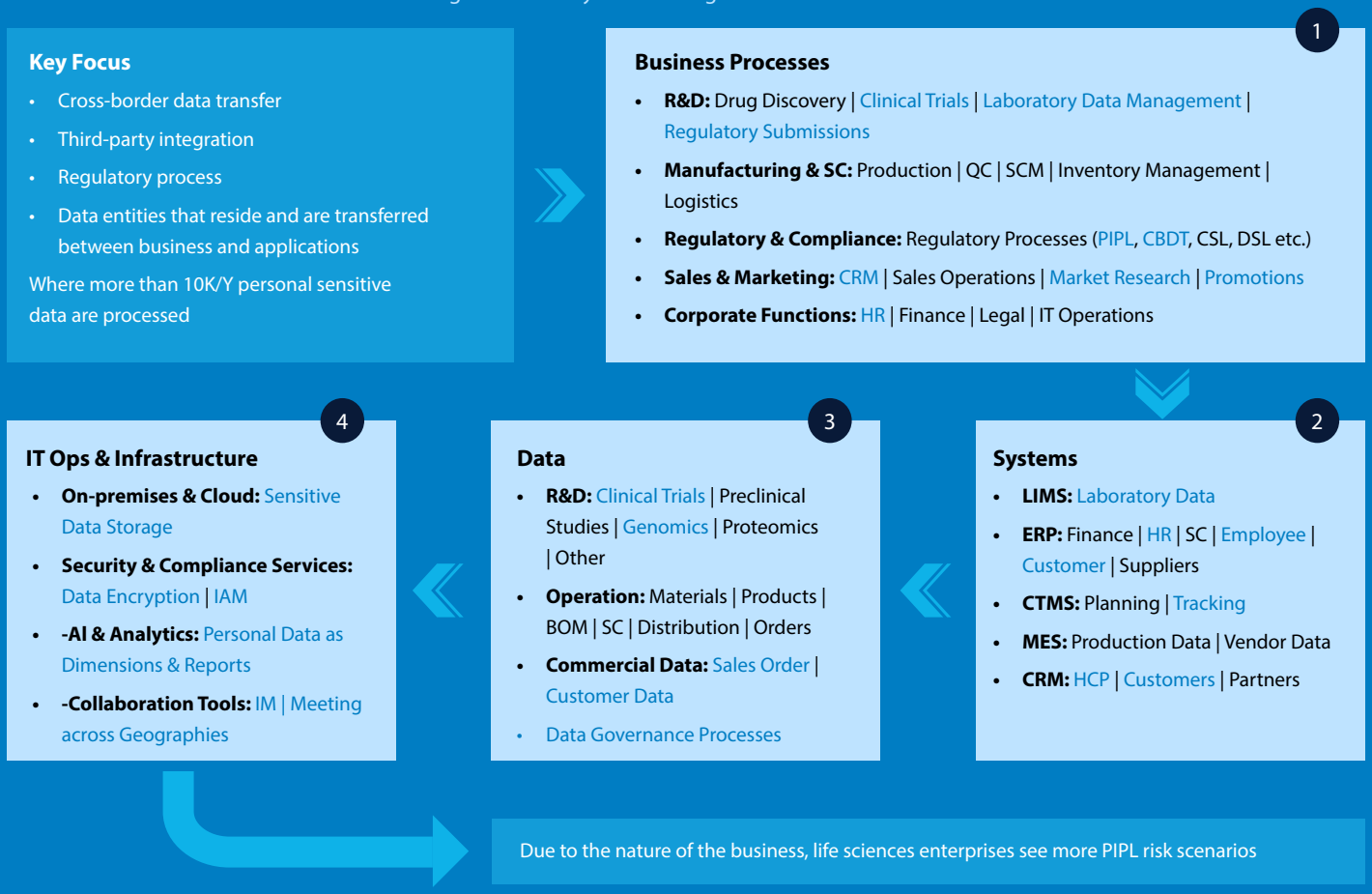
- Unintentional data leaks or non-compliant data collection by employees
- Phishing attacks targeting employees
- Data mishandling during cross-border transfers
- Fail to recognize and report data breaches on time
- Breach of data retention and deletion policies
- Sharing data with unauthorized parties
- Failure to adapt to changing regulations

These risks highlight the importance of establishing comprehensive mitigation strategies that include regular audits, advanced security protocols, and a culture of data protection within the organization.

Systematic Approaches to Identify Risks Using EA Framework

We suggest a structured approach to identifying and managing PIPL risks using an EA framework. By examining core business processes, data types, systems, and IT operations, organizations can align their architecture to comply with regulatory demands while optimizing operations.

Figure 2: Identify Risks through an EA Framework



Business Processes
A range of business processes within life sciences are directly impacted by data protection requirements:

- **Research & Development (R&D)**: Activities like drug discovery, clinical trials, and laboratory data management involve processing sensitive data that must be secured.
- **Manufacturing & SC**: Operational processes like production, quality control, supply chain management, inventory management, and logistics generate substantial data requiring stringent security and privacy controls to comply with PIPL.
- **Regulatory & Compliance**: Managing regulatory processes effectively is crucial and adherence to PIPL, CSL, DSL, and other frameworks requires robust processes and policies.
- **Sales & Marketing**: Functions such as CRM, market research, and promotional activities involve customer data, necessitating careful handling and compliance.
- **Corporate Functions**: Key operations in finance, HR, IT, and legal are integral to enterprise success and must align with data privacy regulations.

Systems

The life sciences industry relies on a complex network of systems that support day-to-day operations, and each of these systems poses unique data protection challenges:

- **Laboratory Information Management Systems (LIMS)**: LIMS handle laboratory data, requiring strict access controls and audit trails.
- **Enterprise Resource Planning (ERP)**: ERP systems encompass finance, HR, supply chain, and customer data, necessitating multi-layered security measures.
- **Clinical Trial Management Systems (CTMS)**: Used to plan and track clinical trials, these systems store sensitive patient and trial data that must remain secure.
- **Manufacturing Execution Systems (MES)**: MES handle sensitive production and vendor data, demanding robust security measures and strict adherence to data privacy regulations.
- **Customer Relationship Management (CRM)**: CRM systems manage data related to HCPs, customers, and partners, highlighting the critical need for robust data privacy protocols and adherence to PIPL requirements.

Data

Data within life sciences organizations spans various domains, each with specific governance requirements:

- **R&D**: Clinical trial and genomic data must be securely managed, with special attention to data sovereignty and cross-border regulations.
- **Operation**: Operational data encompassing materials, products, bills of materials, supply chain, distribution, and orders necessitate robust data security and privacy measures throughout the operational lifecycle.
- **Commercial Data**: Customer and sales order data require stringent data governance and compliance measures to avoid breaches.
- **Data Governance Processes**: Establishing clear data governance processes across these domains enables organizations to better manage data lineage, access, and retention, reducing regulatory risks.

IT Ops & Infrastructure

The backbone of risk management lies in a robust IT infrastructure that supports secure, compliant data handling. Key areas of focus include:

- **On-premises & Cloud Storage**: Sensitive data storage solutions must offer high levels of security and flexibility to meet compliance requirements.
- **Security & Compliance Services**: Data encryption and Identity and Access Management (IAM) are essential to protect personal data and enforce access controls.
- **AI & Analytics**: Leveraging AI to analyze data while protecting personal information requires careful design to prevent unintended disclosures.
- **Collaboration Tools**: Tools for instant messaging and geographically distributed meetings support secure and compliant communication across global teams.

Besides the above analysis, some key scenarios call for more attention in practice:

Cross-border Data Transfers: Life sciences enterprises often engage in global collaborations, necessitating cross-border data flows. Under PIPL, such transfers require stringent security assessments or certifications to ensure the protection of sensitive data. Transferring high volumes of personal data (e.g., over 10,000 sensitive records annually) faces increased scrutiny under PIPL and must be proactive in identifying and mitigating associated risks.

Third-party Integration: Collaborations with external vendors and research partners introduce additional data security risks.

Data Management across Business Applications: Sensitive data entities, such as clinical trial data and genomic information, are utilized across various applications and workflows. Proper governance and security controls are essential to protect data as it moves through multiple systems.

Due to the nature of life sciences operations, particularly the handling of sensitive personal and medical data, these enterprises encounter heightened PIPL compliance challenges. By following a systematic, EA-driven approach to identify and mitigate risks across business processes, systems, data, and IT infrastructure, life sciences companies can create an agile and resilient framework for data protection. Adopting this approach will not only help achieve regulatory compliance but also strengthen the foundation for digital transformation and innovation.

Framework for Mitigating Risks in Compliance

Mitigating compliance risks requires a comprehensive approach that combines policy, procedural, and technological enhancements. Key components of an effective compliance framework include:

Policy Development: Drafting and updating privacy policies that reflect PIPL's requirements.

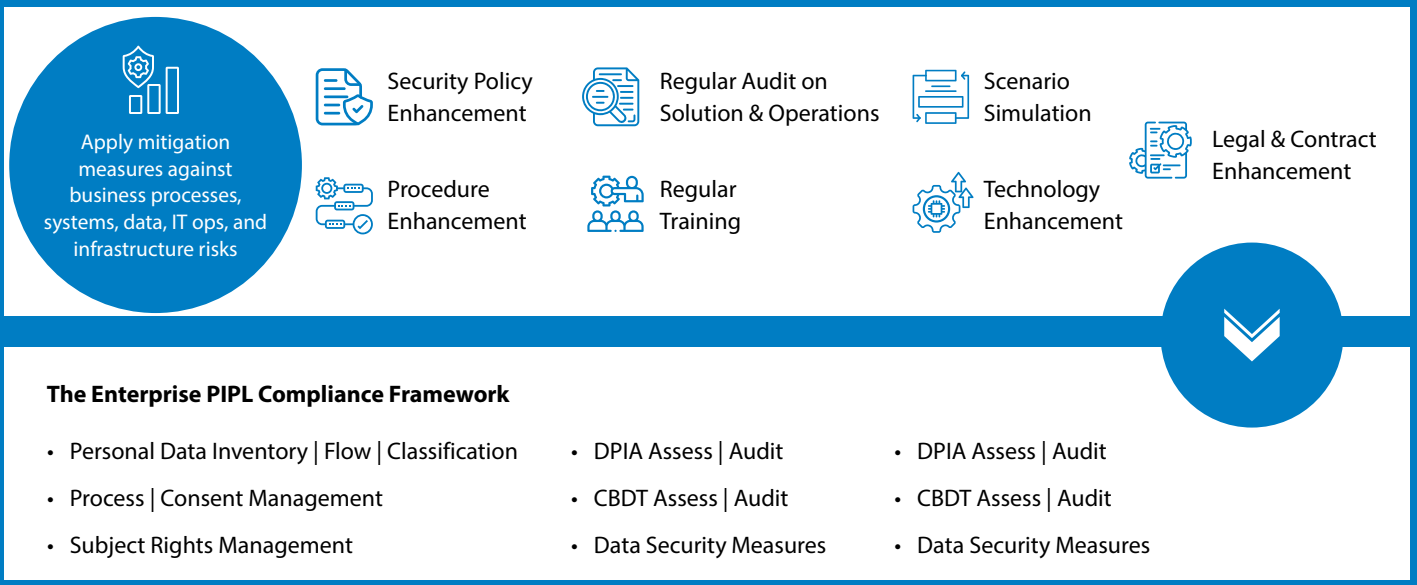
Procedure Enhancement: Developing clear procedures for data processing, consent management, and breach response.

Technology Controls: Implementing advanced security measures, including data encryption, access management, and real-time monitoring.

Employee Training: Ensuring employees understand PIPL requirements and know how to handle personal data responsibly.

These components form the backbone of an effective compliance strategy, helping organizations to adapt quickly to regulatory changes and maintain a high standard of data protection.

Figure 3: A Systematic Approach to Mitigate Risks



Building Compliance with Infosys China Compliance Services

Infosys China offers comprehensive compliance services to help life sciences companies navigate PIPL's complex requirements. By aligning IT assets, security controls, and governance frameworks with regulatory needs, Infosys enables organizations to achieve not only PIPL compliance but also resilience against future regulatory changes. Key services include:

- **Ensuring PIPL Compliance through IT Assets Design, Build & Operation:** Ensuring that the organization's IT infrastructure is optimized for compliance, from data storage solutions to security controls.
- **Compliance Assessment & Remediation:** Providing ongoing monitoring, assessment, and response services to address compliance gaps and adapt to regulatory updates.

These services underscore Infosys China's commitment to delivering compliance solutions that are both sustainable and scalable, enabling life sciences organizations to focus on their core mission while safeguarding their data assets.

Conclusion

The PIPL represents a new era in data protection for China, making compliance not just a legal obligation but also a strategic necessity for life sciences organizations. By building a compliance-oriented culture, adopting systematic methodologies like EA, and leveraging specialized compliance services, organizations can mitigate risks and strengthen their data protection strategies. Infosys China's comprehensive approach enables life sciences companies to navigate the complexities of PIPL compliance, ensuring data privacy, legal alignment, and operational efficiency in the face of stringent regulations.

Authors

Samxuan Wang
Chief Technology Architect
Head of Strategy Technology Group,
Infosys China

The goal of this team is to develop and optimize architectural capabilities at the enterprise, solution, and technology levels. The team supports the delivery services at different stages – IT planning, applications, data and technology solutions, digital solutions, architecture governance, and more. The team focuses on digital transformation and enterprise modernization journeys, AI, cloud migration, data analytics, mobile technology etc. In addition to cloud-native solutions, application architecture, and big data capabilities, the team also works on end-to-end solutions for different industries. These solutions require building, maintaining, and governing the enterprise architecture, as well as delivering technology implementations to ensure that enterprise business transformation is successful.

Md. Arif Khan
Group Project Manager, Infosys &
Delivery Anchor
for Life Sciences and Digital
Experience Portfolios,
Infosys China

He is responsible for Business Operations and Service Delivery for life sciences and digital experience for clients at Infosys China. He is a technology enthusiast with passion for AI, mobility, and automation-led digital service offerings. With over 20 years of experience at Infosys, he has been servicing clients across multiple industry segments. Arif is based in Shanghai, China.

For more information, contact askus@infosys.com

Infosys®
Navigate your next