如何管理生命科学行业的PIPL合规性

摘要

随着中国《个人信息保护法》（PIPL）对数据隐私执行严格的指导方针，合规性已成为生命科学组织面临的重大挑战。我们基于自己的业务实践、结合对PIPL的理解，在本文中探讨了 PIPL 的影响、相关风险，以及生命科学公司如何利用结构化方法和合规框架（如企业架构—EA）来构建安全、合规的系统。通过这些方法，在Infosys中国合规服务的支持下，组织可以降低风险并为数据隐私和安全奠定坚实的基础。

Infosys®
Navigate your next

引言：

遵守 PIPL 的必要性

生命科学领域的快速数字化转型为数据驱动的洞察、个性化医疗和高效的医疗保健交付开辟了新的途径。然而，这种转变也带来了挑战，尤其是在数据隐私方面，因为组织会收集大量敏感的个人数据。中国《个人信息保护法》（PIPL）的出台要求制定更严格的数据隐私法规，如果组织不遵守，可能会受到严厉处罚、甚至威胁到业务的开展。对于经常处理高度敏感的健康和遗传数据的生命科学公司来说，PIPL合规性至关重要——这不仅是为了避免法律后果，也是为了维护公众信任和维护道德标准。

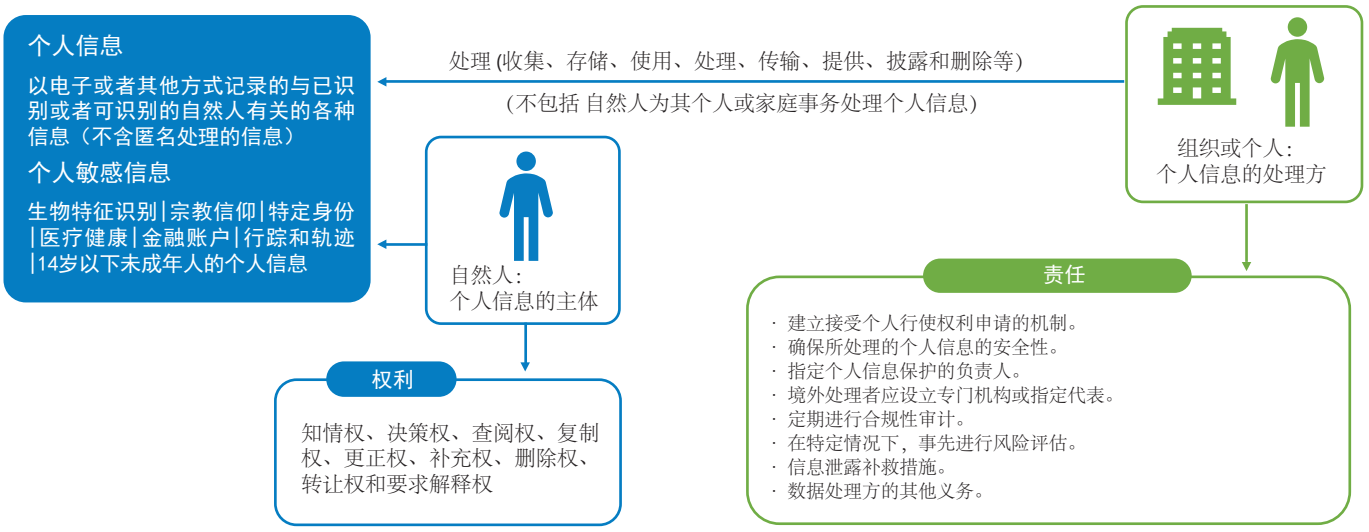
对中国《个人信息保护法》的基本认识 – 概述

首先，PIPL为规范中国境内的个人数据处理提供了一个全面的框架。该法律定义了两种类型的信息：

1. 个人信息：个人信息是指以电子方式或其他方式记录的与已识别或可识别的在世个人相关的数据（与GDPR类似，匿名数据在GDPR下不被视为PI）。
2. 敏感个人信息：一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

此外，PIPL还概述了数据主体的权利（例如访问、更正和删除其数据的权利）以及组织的义务（例如确保数据处理的透明度，在必要时获得同意，并采取安全措施来保护个人数据等）。该框架不仅适用于在中国境内运营的公司，也适用于处理中国个人数据的外国公司，使其影响范围广泛。

图 1 对中国 PIPL 的基本认识 – 概述



此外，其他相关的法律包括：2017年6月1日，《中华人民共和国网络安全法》（CSL）生效，要求采用多级保护计划（MLPS）进行网络安全保护，以及为关键信息基础设施提供额外的保护。2021年9月1日，《中华人民共和国数据安全法》（DSL）生效，要求建立数据分类分级保护制度，对数据进行分类、分级保护，以及对关键数据处理者应对其数据处理活动进行风险评估。

PIPL 对企业提出的关键要求

PIPL 对生命科学公司的影响涵盖所有运营领域，尤其是在数据治理、IT 安全和合规性管理方面：

- 内容：PIPL 强制要求保护个人数据，强调保护敏感数据（如医疗记录、基因数据和患者信息）的必要性。
- 主体：处理中国个人数据的组织必须遵守 PIPL 的要求，即使它们在中国境外运营。
- 地点：该法律适用于中国境内，但也适用于处理中国公民数据的外国实体。

这些领域突出了《个保法》对企业运营的关键要求：

数据收集和同意：要求组织明确同意个人收集数据，以及 IT 系统来管理此同意。

安全措施和泄露通知：要求采用技术措施来保护数据和报告违规行为，重点是安全技术和事件响应。

对组织的培训和赋能：了解风险，对不合规行为实施严厉处罚，例如罚款和停业。并且结合业务岗位分配职责。

数据最小化和目的限制：仅应出于特定目的收集必要的数据，突出数据治理的必要性。

数据传输和跨境限制：跨境数据传输需要安全评估或认证，并有系统确保数据流合规。

个人权利：个人有权访问、更正和删除数据，这需要支持性的流程和系统。

医疗行业中 PIPL合规相关的风险模式和场景

不遵守 PIPL 会使生命科学公司面临各种风险，包括经济处罚、声誉损害和运营中断。常见的风险场景包括：

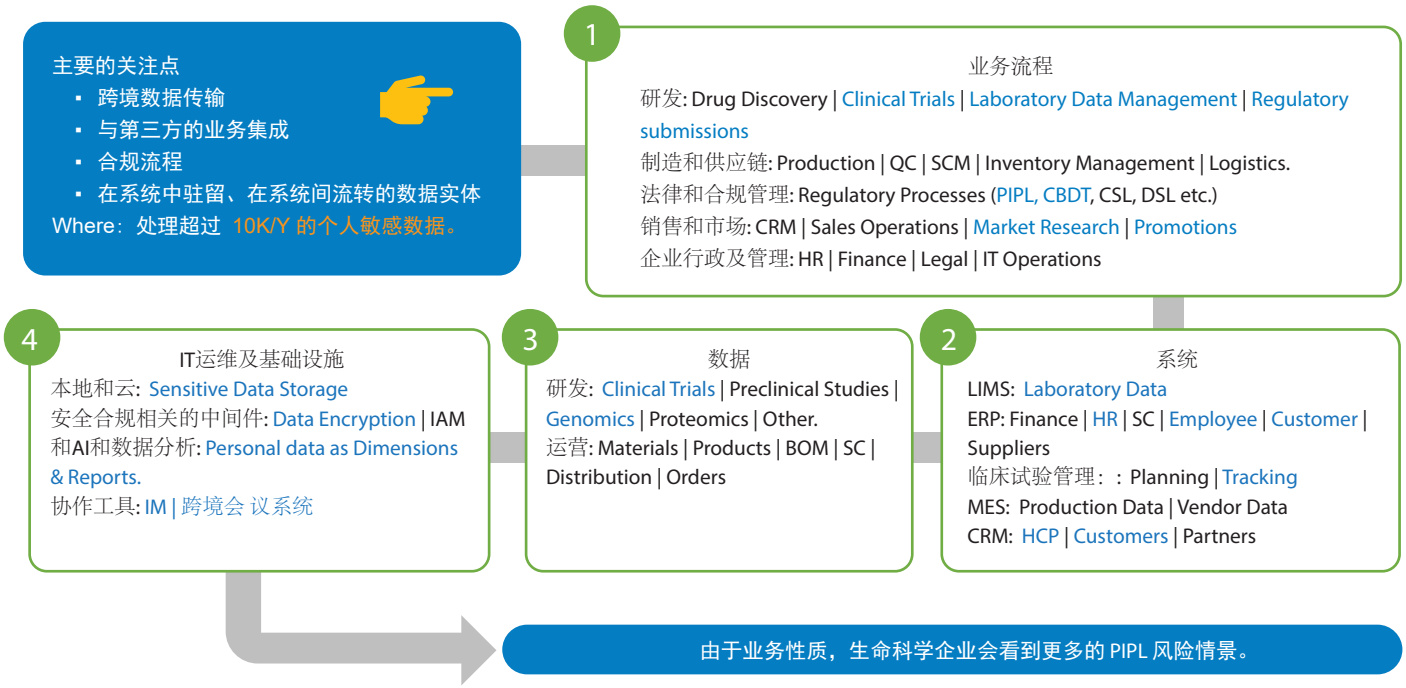
- 针对征得主体同意缺乏相关业务能力：
  - 临床试验和研究数据。
  - 用于药品营销或市场研究的患者数据。
  - 与医疗保健提供商和合作伙伴共享数据。
  - 基因组和遗传数据处理。
  - 通过移动或可穿戴设备收集的个人健康数据。
- 数据安全措施不足：
  - 未经授权访问个人健康数据。
  - 不遵守数据最小化和目的限制原则。
  - 第三方数据安全评估不足。
  - 对数据进行匿名化/去标识化处理的措施不足。
  - 缺乏事件响应和违规通知
  - 应用程序、中间件、第三方云服务和基础设施中的漏洞。
- 未能实施数据主体权利：
  - 未能响应数据访问请求。
  - 无法满足数据更正请求。
  - 延迟处理数据删除请求。
  - 不遵守撤回同意。
  - 数据处理的透明度不足。
  - 缺乏响应和处理的自动化或机制。
- 跨境数据传输
  - 涉及国际研究的临床试验。
  - 与全球合作伙伴共享医疗数据。
  - 将数据分析外包给海外服务提供商。
  - 使用国际云服务。
  - 为国际研究输出基因数据。
  - 并购中的跨境数据传输。
- 第三方风险管理：
  - 与第三方的数据处理协议和疏忽不足。
  - 在跨境研究中向第三方传输数据。
  - 对云服务的安全监控不足。
  - 未经同意与营销合作伙伴共享数。
  - 未能实施必要的数据匿名化。
  - 将数据处理外包给第三方前后缺乏评估过程。
- 缺乏员工培训和意识：
  - 员工无意间泄露数据或采取不合规的数据收集行为。
  - 针对员工的网络钓鱼攻击。
  - 跨境传输过程中的不当的数据处理。
  - 未能及时识别和报告数据泄露。
  - 违反数据保留和删除制度。
  - 与未经授权的各方共享数据。
  - 未能适应不断变化的法规。

这些风险凸显了建立全面的风险管理制度的重要性，这些制度包括定期审计、高级安全协议和组织内的数据保护文化。

使用 EA 框架识别风险的系统方法

使用企业架构（EA）框架进行风险的识别，是一种结构化的方法，可用于系统地评估、识别和减轻合规性风险。EA框架允许医疗行业的企业系统地描绘出数据、系统和流程环境，可以确保合规性工作与业务目标保持一致，同时优化运营。

图2 通过EA框架识别风险



重点领域包括：

1. 生命科学领域的一系列业务流程直接受到数据保护要求的影响，例如：

研发（R&D）：药物发现、临床试验和实验室数据管理这样的活动涉及处理必须保护的敏感数据。

监管与合规：有效管理监管流程是合规工作的核心。需要针对 PIPL、CSL、DSL 和其他合规要求对流程进行优化。

销售和营销：CRM、市场研究和促销活动等功能涉及客户数据，需要谨慎处理和合规。

企业职能：财务、人力资源、IT 和法律方面的关键运营是企业成功不可或缺的一部分，必须遵守数据隐私法规。

2.支持业务流程的应用程序。生命科学行业依赖于支持日常运营的复杂系统网络，而这些重点系统中的每一个都带来了独特的数据保护挑战：

实验室信息管理系统（LIMS）：处理实验室数据，需要严格的访问控制和审计跟踪。

企业资源规划（ERP）：包括财务、人力资源、供应链和客户数据，需要多层安全措施。

临床试验管理系统：这些系统用于规划和跟踪临床试验，存储必须保持安全的敏感患者和试验数据。

客户关系管理（CRM）：管理 HCP 和客户数据，强调严格的数据隐私协议的必要性。

3. 数据架构及其治理。生命科学组织中的数据跨越各个领域，每个领域都有特定的治理要求：

研发数据：临床试验和基因组数据必须得到安全管理，需要特别注意数据主权和跨境法规。

商业数据：客户和销售订单数据需要严格的数据治理和合规性措施，以避免泄露。

跨这些域建立清晰的数据治理流程使组织能够更好地管理数据血缘、访问和存储，从而降低监管风险。

4. 用于数据保护的 IT 运营和基础设施。风险管理的支柱在于强大的 IT 基础设施，该基础设施支持安全、合规的数据处理。重点领域包括：

本地和云存储：敏感数据存储解决方案必须提供高水平的安全性和灵活性，以满足合规性要求。

安全与合规服务：数据加密和（IAM）对于保护个人数据和实施访问控制至关重要。

AI 和分析：利用 AI 分析数据，同时保护个人信息，需要精心设计以防止意外泄露。

协作工具：即时消息和跨国会议工具支持全球团队之间安全合规的通信可能存在薄弱环节。

除了上述分析外，从场景角度，一些情况在实践中需要更多关注：

跨境数据传输：生命科学企业经常参与全球合作、并且需要跨境数据流动。根据 PIPL，此类传输需要严格的安全评估或认证，以确保敏感数据得到保护。特别地，传输大量个人数据（例如，每年超过 10,000 条敏感记录）面临更严格的审查，必须主动识别和减轻相关风险。

第三方集成：与外部供应商和研究合作伙伴的合作会带来额外的数据安全风险。

跨业务应用程序的数据管理：敏感数据实体（例如临床试验数据和基因组信息）可能会用于各种应用程序和工作流。适当的治理和安全控制对于保护在多个系统中移动的数据至关重要。

由于生命科学运营的性质，尤其是需要处理敏感的个人和医疗数据，这些企业面临着更高的 PIPL 合规性挑战。通过遵循 EA 驱动的系统化方法来识别和降低业务流程、系统、数据和 IT 基础设施中的风险，生命科学公司可以创建一个敏捷且有弹性的数据保护框架。采用这种方法不仅有助于实现监管合规性，还可以加强数字化转型和创新的基础。

使用合规性框架管理风险的系统方法

降低合规性风险需要一种将制度、流程和技术增强相结合的综合方法。有效的合规性框架的关键组成部分包括：

· 制度制定：起草和更新反映 PIPL 要求的隐私制度。

· 流程增强：为数据处理、同意管理和违规响应制定明确的流程。

· 技术控制：实施高级安全措施，包括数据加密、访问管理和实时监控。

· 员工培训：确保员工了解 PIPL 要求并知道如何负责任地处理个人数据。

以上各方面构成了有效合规性策略的支柱，可帮助组织快速适应监管变化并保持高标准的数据保护。

图 3 风险管理的系统化方法

使用 Infosys 中国的合规服务确保合规性

Infosys 中国提供全面的合规服务，帮助生命科学公司应对 PIPL 的复杂要求。通过将 IT 资产、安全控制和治理框架与监管需求保持一致，Infosys 使组织不仅能够实现 PIPL 合规性，而且能够抵御未来的监管变化。主要服务包括：

- 通过 IT 设计、构建和运营确保 PIPL 合规性：确保组织的 IT 基础设施从数据存储解决方案到安全控制都针对合规性进行了优化。
- 合规性评估和补救：提供持续的监控、评估和响应服务，以解决合规性差距并适应法规更新。
- 框架定制化：定制合规框架以符合生命科学行业的特定需求，并纳入数据保护和隐私的最佳实践。

这些服务凸显了Infosys中国致力于提供可持续且可扩展的合规解决方案的承诺，使生命科学组织能够专注于其核心使命，同时保护其数据资产。

结论

PIPL代表了中国数据保护的新时代，使合规不仅成为一项法律义务，而且是生命科学组织的战略必要条件。通过建立以合规性为导向的文化，采用企业架构等系统方法，并利用专门的合规性服务，组织可以降低风险并加强其数据保护策略。Infosys中国的综合方法使生命科学公司能够驾驭 PIPL 合规性的复杂性，在面对严格的法规时确保数据隐私和运营效率。

关于作者

王宣

印孚瑟斯（Infosys）首席技术架构师，Infosys中国区战略技术组责人

这个团队的目标是在企业、解决方案和技术层面发展和优化架构能力。该团队在不同阶段支持我们的交付业务——包括IT规划、应用程序、数据和技术解决方案、数字化技术、架构治理等等。该团队专注于数字化转型和企业现代化旅程、AI、云迁移、数据分析、移动技术等尖端技术的应用。除了云原生解决方案、应用架构、大数据能力外，他们还提供针对不同行业的端到端的解决方案。这些解决方案需要构建、维护和治理企业架构、以及交付技术实现方案，以确保满足业务转型的需要。

Md. Arif Khan

印孚瑟斯（Infosys）项目经理，Infosys中国生命科学和数字体验产品组合交付负责人

Arif目前就职于Infosys中国上海分公司。他主要负责Infosys中国生命科学和数字体验客户的业务运营和服务交付。他是一名技术爱好者，对人工智能、移动和自动化主导的数字服务产品充满热情。他在Infosys拥有超过20年的经验，一直为多个行业的客户提供服务。

For more information, contact askus@infosys.com

Infosys®
Navigate your next