远大医药集团有限公司
信息安全与隐私保护政策

第一章　总则

第一条　为进一步保障远大医药集团有限公司及下属成员企业（以下简称“远大医药”“公司”或“我们”）的信息安全与隐私保护，确保数据的机密性、完整性和可用性，防范信息泄露、篡改和丢失等风险，同时要求承包商、供应商及商业伙伴遵守同等或更高标准的信息安全与隐私保护要求，本公司依据《网络安全法》《数据安全法》《个人信息保护法》《数据出境安全评估办法》《个人信息出境标准合同办法》等相关法律法规，特制定本政策。

第二条　本政策适用于公司及所有下属成员企业的全体员工、承包商、供应商、商业合作伙伴及相关第三方，涵盖所有与公司业务相关的信息系统、数据处理活动及信息资产。

第二章　信息安全与隐私保护原则

第三条　远大医药在开展一切业务活动的过程中应遵循以下原则：

（一）合规合法原则。公司严格遵守中国及业务运营所在国家或地区有关网络安全、数据安全、个人信息保护及相关法律法规，包括但不限于《网络安全法》《数据安全法》《个人信息保护法》《个人信息出境安全评

估办法》等，确保所有信息处理活动合法合规。

（二） 最小必要与目的限定原则。公司仅在实现特定业务目的所必需的范围内收集、使用、存储和处理个人信息与数据，不超出授权范围，不用于无关用途，确保数据处理行为具有明确、合法、正当的目的。

（三） 零容忍原则。公司明确禁止任何违反隐私政策的行为，对发生数据泄露、未经授权访问、滥用个人信息等违规行为采取纪律处分措施。

第三章　信息安全保护承诺

第四条　远大医药高度重视信息安全保护，努力确保公司信息资产的机密性、完整性和可用性。公司承诺在所有业务活动中落实以下信息安全保护原则与措施

（一） 持续改进信息安全体系。公司建立并不断完善信息安全管理体系，定期评估、更新和优化安全策略、技术措施与管理流程，推动安全能力的持续演进，以应对不断变化的网络威胁环境。

（二） 确保数据的完整性。公司采取有效技术和管理措施，防止数据被篡改、泄露、损毁或非法访问，对敏感数据实施加密管理，达到对敏感数据的技术防控，保障数据在生成、存储、传输、使用和销毁各环节的完整、准确与安全。

（三） 主动监控并及时响应信息安全威胁。公司部署先进的威胁检测与响应机制，持续监控网络与系统活动，对异常行为、安全事件和潜在风险进行及时识别、分析与处置，最大限度降低安全事件影响。当发生信息安全事件时，与受影响的相关方保持透明沟通，传达为修复漏洞和防范未来风险所采取的措施。

（四） 建立全员信息安全责任机制。公司信息安全管理制度适用于全体员工，明确各级员工在信息安全中的职责与义务，通过保密协议、培训考核与问责机制，强化全员安全意识，遵循“系统策划，全面控制；信息安全，人人有责；灾难预防，永续运营；检查测评，持续改进”的策略方针。

（五） 要求第三方（如供应商、商业伙伴）遵守信息安全标准。公司要求所有与公司开展业务合作的第三方在数据处理、系统接入、服务提供等环节，必须遵守公司设定的信息安全与隐私保护标准。同时所有第三方需通过合同承诺遵守与本政策同等或更高标准的数据保护义务，违规行为将终止合作并追究责任。

第四章　隐私保护

第五条　远大医药收集的个人信息包括以下类型：

（一） 数据主体的个人身份和联系信息，如姓名、电子邮件

地址、电话号码、所在国家和城市

（二） 就业信息，如雇主、工作职位和工作履历

（三） 通信中获取的数据主体信息（如评论、问题、反馈和使用网站功能过程中提供的其他内容）

（四） 不良反应信息，如年龄、体重、既往病史、过敏史、不良反应描述和使用药品情况等

（五） 其他为履行法定义务或开展特定业务所必需的个人敏感信息，例如临床试验相关数据、患者健康档案信息、药物警戒报告中的个人身份与健康信息等。

第六条　公司可能将数据主体的信息用于以下用途：

（一） 查阅数据主体的意见或问题，并向其提供相应的服务支持

（二） 执行公司网站的条款与政策

（三） 处理和回复数据主体的请求、问询、申请、投诉和反馈

（四） 提供支持并回应数据主体的请求、反馈和问询

（五） 监测、操作、维护和管理公司网站

（六） 处理和解决公司网站的技术问题和故障

（七） 确保公司网站有效和高效地运行

（八） 发现、防止或以其他方式应对安全、欺诈或技术相关问题

（九） 改进和提升公司网站及相关服务的功能与性能；

（十） 妥善管理和维护公司与用户之间的关系

（十一） 支持公司的日常业务管理

（十二） 保护、执行或维护公司的合法权利与利益（包括针对违反公司网站条款与条件行为所享有的权利与利益）

在获得数据主体同意，且法律允许的情况下，公司还可能根据事先向数据主体披露的其他目的对信息进行处理。

第七条 数据主体可自主决定其个人数据的收集、使用、留存及处理方式，并享有以下权利：

（一） 数据访问权。数据主体有权要求我们确认我们是否处理其个人信息，并要求我们提供其个人信息的副本。

（二） 数据更正权。如果我们所收集的数据主体的任何个人信息不完整或不准确，数据主体可以要求我们更正或更新这些信息。

（三） 数据删除权。在特定情况下，数据主体可以要求我们删除全部或部分个人信息：

- 我们对个人信息的处理违反适用法律、行政法规；
- 未经数据主体同意，收集或使用了其个人信息；
- 我们对数据主体个人信息的处理违反了我们与数据主体之间的约定；

- 处理数据主体个人信息的目的已实现、无法实现或者为实现处理目的不再必要；或
- 数据主体已经撤回对我们处理其个人信息的授权同意。

（四） 选择同意。对于敏感数据处理或非必要用途，必须向数据主体明确告知处理的必要性及对个人权益的影响，并获得用户明确、主动的“选择同意”（Opt-in Consent），禁止默认勾选或强制同意。

（五） 撤回同意。如果我们对个人信息的处理是基于数据主体的同意，数据主体有权在任何时候撤回同意。

（六） 可携带权。数据主体有权以结构化的、常用的且机器可读的格式，接收其提供给我们的个人信息，并且有权将该个人信息传输给另一个实体。

（七） 知情权。数据主体有权了解我们处理其个人信息的目的、方式、范围、保存期限及第三方共享情况等信息。

第八条 我们将在个人信息用于提供公司网站、相关服务及经营业务所需的时间内，或在实现信息收集目的所必需的期限内，保留该等信息。公司视所收集信息的性质，在信息保存 18 至 36 个月后将信息删除。

第九条 公司依据本隐私政策实施安全措施，并建立实体、电子及管理层面的保护流程，以保障所处理的用户信息

的安全。

第十条　公司仅在履行合同、获得用户同意、遵守法律或应对安全事件等合法情形下向第三方（服务提供商、关联方、执法机构和主管部门等）披露数据。所以第三方必须遵守公司设定的信息安全与隐私保护标准。

第十一条　公司进行任何形式的数据跨境传输（包括向境外接收方提供个人信息、公司重要数据、技术秘密等资产），均将严格遵守数据出境地和数据接收地所适用的法律法规。涉及个人信息出境的，将依法向个人履行详尽告知义务（包括但不限于境外接收方信息、处理目的、方式、种类及行使权利的方式等），并获取个人的单独同意。同时公司将根据法律法规及业务环境的变化及时更新管理措施。

第五章　负责任的人工智能使用

第十二条　远大医药致力于以符合公司道德准则的方式负责任地运用人工智能（AI），尊重每位个体的权利与尊严，在业务实践中践行非歧视、隐私保护与公平对待。公司相信AI能够为客户、员工及社区创造显著价值，但其发展与应用必须始终以坚实的道德准则与适用法律法规为指引。公司在人工智能的使用和/或开发中承诺遵循以下原则：

（一） 尊重数据隐私。在人工智能的使用和/或开发中严格保护个人数据的隐私与安全，遵守适用的数据保护法律法规，并以负责任且透明的方式管理个人信息。

（二） 保障网络安全。在人工智能使用和/或开发过程中，于系统中内嵌安全与保障机制，对系统进行严格测试与持续监控，防范网络威胁、滥用及意外后果。

（三） 避免潜在偏见。主动识别并缓解人工智能使用和/或开发中可能产生的偏见，尤其关注各运营所在地法律法规所保护的个人特征（如种族、性别、年龄等），一旦发现偏见或歧视性结果立即采取纠正措施。

（四） 保持人类参与与人工干预。在关键决策中确保有人工介入，特别是在决策对个人产生重大影响时，由人主导最终判断与合规审查，并允许在必要时进行人工干预。

（五） 确保透明性与可解释性。在实际可行的情况下，提供清晰、易懂的说明，解释人工智能系统如何运作及作出决策，确保人工智能系统的透明性以及其生成结果/决策的可解释性。

（六） 明确责任归属。为人工智能模型/工具所产生的结果建立清晰的问责机制，明确相关结果与决策的责任归属，并设有相应的治理结构与应对流程，以妥善处理可能出现的意外后果或损害。

（七） 界定清晰的应用边界。明确界定人工智能可为与不可为的清晰边界，规范人工智能的适用场景与使用方式，防止超范围或不当使用。

（八） 关注生态足迹。要求自有及第三方的人工智能数据中心/模型具有较低的生态足迹，在技术选型与部署中兼顾能效与可持续发展。

（九） 禁止使用违规的人工智能系统。公司不使用/部署涉及操纵行为、利用人群脆弱性（漏洞）、社会评分或未经授权的生物识别监控的人工智能系统，公司使用人工智能系统时，应当遵守包括《生成式人工智能服务管理暂行办法》在内的中国法律法规及适用法律的规定。

第六章　监督

第十三条　公司信息管理部负责组织并指导本政策在公司内部的日常运行，确保本政策实施的有效性。远大医药董事会对隐私政策的执行情况及关键绩效进行监督。

第十四条　公司将隐私政策管理融入集团层面的合规管理体系，对隐私政策合规情况开展内部审计，并在必要时开展第三方审计。

第七章　附则

第十五条　本政策未尽事宜，或者与有关法律、法规、规范性文件相悖的，按有关法律、法规、规范性文件执行。

第十六条　本政策由公司 ESG 工作小组制订、修订并解释，自发布之日起生效。