基于隐私计算的医疗 AI 软件开发及合规性研究

张跃华[1] 张南极[2] 赖俊朴[3]
1.浙江飞图影像科技有限公司 311100；
2.浙江零跑科技股份有限公司 311100；3.杭州科腾生物制品有限公司 310000

【摘 要】本研究聚焦隐私计算技术在医疗AI软件开发中的融合应用与合规体系构建，结合医疗数据的敏感性与AI技术的应用特性，探索适配医疗场景的隐私计算技术落地路径，优化医疗AI软件的开发流程与技术架构。同时，从法律、行业规范、技术应用维度剖析医疗AI软件开发的合规要点，搭建全流程合规管控体系，解决数据利用与隐私保护的核心矛盾，为医疗AI产业的规范化、可持续发展提供理论支撑与实践参考。

【关键词】隐私计算；医疗AI软件；软件开发；合规管控；数据隐私保护

Research on Medical AI Software Development and Compliance Based on Privacy Computing

Zhang Yuehua[1] Zhang Nanji[2] Lai Junpu[3]
1.Zhejiang Feitu Imaging Technology Co.，Ltd. 311100；
2.Zhejiang Lingpao Technology Co.，Ltd. 311100；3.Hangzhou Keton Biological Products Co.，Ltd. 310000

【Abstract】This study focuses on the integration and application of privacy-preserving computing （PPC） technology in medical AI software development，along with the establishment of a compliance framework. By considering the sensitivity of medical data and the characteristics of AI technology，it explores practical pathways for implementing PPC in medical scenarios，optimizing the development process and technical architecture of medical AI software. Additionally，it analyzes compliance considerations in medical AI software development from legal，industry standard，and technical application perspectives，establishing a comprehensive compliance management system. This addresses the core conflict between data utilization and privacy protection，providing theoretical support and practical references for the standardized and sustainable development of the medical AI industry.

【Key words】Privacy computing；Medical AI software；Software development；Compliance management；Data privacy protection

1 引言

医疗健康领域的数字化转型推动 AI 技术深度渗透，临床诊断、疾病预测、药物研发等场景的 AI 应用均以海量医疗数据为核心基础，但医疗数据包含个人生理、病理等敏感信息，数据安全与隐私保护成为行业发展的核心桎梏。隐私计算技术通过在数据不可见、不可泄露的前提下实现数据价值挖掘，为医疗 AI 开发打破数据壁垒提供了技术可能。与此同时，医疗 AI 软件作为医疗科技产品，其开发、测试、落地全流程需契合多领域合规要求。本研究围绕隐私计算与医疗 AI 软件开发的融合逻辑展开分析，梳理开发各环节的合规痛点与管控策略，旨在实现技术应用与合规要求的双向适配，推动医疗 AI 技术在合法合规的前提下充分释放数据价值。

2 隐私计算与医疗 AI 软件开发的融合逻辑

2.1 医疗 AI 软件开发的核心数据需求与技术痛点

医疗 AI 软件的功能实现依赖多源异构医疗数据的训练与验证，涵盖电子健康档案、检验检测报告、医学影像、基因测序数据等，这类数据的完整性、多样性直接决定 AI 模型的精度与泛化能力。但当前医疗数据存在跨机构流通难、数据孤岛现象突出的问题，医疗机构因数据隐私保护要求与责任顾虑，难以实现数据开放共享，导致 AI 模型训练数据量不足、样本单一，制约模型性能提升。同时，医疗 AI 软件开发过程中，数据采集、清洗、模型训练、推理部署各环节均存在数据泄露风险，传统的加密存储、访问控制等方式难以兼顾数据利用效率与隐私保护，无法满足 AI 模型对数据实时调用、多维度分析的需求，成为医疗 AI 软件开发的核心技术痛点。

2.2 隐私计算适配医疗 AI 软件开发的技术特性

隐私计算技术体系包含联邦学习、安全多方计算、差分隐私、同态加密等核心技术，各技术具备的非接触式数据利用特性与医疗 AI 软件开发的需求高度契合。联邦学习支持

多机构在不共享原始数据的前提下，联合开展 AI 模型训练，实现数据“可用不可见”，适配医疗机构跨域协作开发医疗 AI 软件的场景；差分隐私通过对数据添加噪声实现隐私保护，可应用于医疗 AI 软件的训练数据预处理与推理结果输出环节，在保证数据可用性的同时，有效规避个体信息泄露；安全多方计算能够实现多参与方在数据隐私保护的前提下完成联合计算，适用于医疗 AI 模型的多源数据融合分析场景。

3 基于隐私计算的医疗 AI 软件开发全流程设计

3.1 需求分析与技术选型阶段的融合设计

医疗 AI 软件开发的需求分析阶段，需同时兼顾功能需求、性能需求与隐私保护需求，通过与医疗机构、临床医生、医疗信息化专家的多维度沟通，明确软件的应用场景、服务对象、核心功能，同时梳理软件开发所需的数据类型、数据来源、数据规模，结合数据敏感程度划定隐私保护等级。技术选型阶段，以需求分析结果为依据，开展隐私计算技术的针对性选型，若软件开发涉及多医疗机构联合建模，优先选用联邦学习技术，并搭配边缘计算实现终端数据的本地化处理；若软件需对原始医疗数据进行直接分析，选用差分隐私技术进行数据脱敏；若软件涉及多参与方的联合数据计算与模型验证，采用安全多方计算技术。同时，结合 AI 技术体系，将隐私计算技术与深度学习、机器学习、计算机视觉等技术进行融合选型，保障技术体系的兼容性与适配性。

3.2 数据处理阶段的隐私计算技术应用

数据处理是医疗 AI 软件开发的基础环节，涵盖数据采集、数据清洗、数据标注、数据划分等步骤，各步骤均需嵌入隐私计算技术实现全流程隐私保护。数据采集环节，基于隐私计算技术搭建多源数据采集平台，通过联邦采集模式实现不同医疗机构、不同数据终端的非接触式数据采集，采集过程中对数据进行实时加密处理，避免原始数据的传输与泄露；数据清洗环节，利用安全多方计算技术实现多参与方联合数据清洗，在不获取原始数据的前提下，完成数据缺失值填充、异常值剔除、数据格式统一等操作，保证清洗后数据的有效性；数据标注环节，采用联邦标注模式，由各医疗机构的专业人员在本地完成数据标注，通过隐私计算技术实现标注结果的联合汇总与共享，避免标注过程中敏感数据的暴露；数据划分环节，结合差分隐私技术对划分后的训练集、验证集、测试集添加个性化噪声，根据数据隐私保护等级调整噪声强度，在保护数据隐私的同时，保证数据对 AI 模型训练的支撑作用。

4 医疗 AI 软件开发的合规维度与核心要求

4.1 法律层面的合规核心要求

医疗 AI 软件开发的法律合规以数据安全与隐私保护相关法律法规为核心，同时契合医疗行业专门性法律规范的要求。在数据利用方面，需严格遵循《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国网络安全法》的规定，明确医疗数据的分级分类标准，对敏感个人信息的采集、使用需取得个人的单独同意，同时履行数据采集、使用的告知义务，保障数据主体的知情权、决定权、删除权等合法权利。在医疗行业规范方面，需契合《中华人民共和国基本医疗卫生与健康促进法》《医疗机构管理条例》的要求，医疗 AI 软件若涉及临床诊断、治疗建议等医疗服务功能，需符合医疗服务的规范与标准，不得超出医疗机构的服务范围与执业资质。此外，医疗 AI 软件开发过程中涉及的跨机构数据合作、第三方技术服务，需签订合法有效的合作协议，明确各方的权利与义务，划定数据隐私保护的责任边界。

4.2 行业规范层面的合规核心要求

医疗 AI 软件作为医疗科技产品，其开发、测试、注册、落地需遵循医疗行业与人工智能行业的双重规范要求。医疗行业层面，国家药品监督管理局发布的《医疗器械人工智能软件注册审查指导原则》为医疗 AI 软件的注册审批提供了明确规范，软件开发需契合“算法透明、可解释、可追溯”的要求，模型的训练数据、训练过程、验证结果需形成完整的技术文档，保障软件的安全性、有效性与可靠性。人工智能行业层面，需遵循《新一代人工智能伦理规范》《人工智能算法推荐系统基本要求》等规范，医疗 AI 软件开发需坚持“以人为本、生命至上”的伦理原则，避免算法歧视、算法黑箱等问题，同时保障 AI 模型的决策可解释性，临床应用场景中需为医生提供明确的决策依据，不得完全替代医生的临床判断。此外，医疗 AI 软件开发需遵循医疗数据管理的行业规范，如《电子病历应用管理规范》《健康医疗大数据标准管理办法》，保障数据采集、处理、利用的标准化与规范化。

5 基于隐私计算的医疗 AI 软件开发合规管控体系构建

5.1 全流程合规管控体系的整体框架

基于隐私计算的医疗 AI 软件开发合规管控体系，以“事前预防、事中管控、事后追溯”为核心逻辑，搭建“组织管控、制度管控、技术管控、人员管控”的四维整体框架，实现合规要求与软件开发各环节的深度融合。组织管控层面，成立专门的合规管理部门，配备医疗、法律、人工智能、数据安全等领域的专业人员，统筹软件开发全过程的合规管理工作，明确各部门、各岗位的合规职责；制度管控层面，制

定完善的合规管理制度，涵盖数据管理、技术应用、模型开发、产品部署等各环节的合规规范，形成标准化的合规操作流程；技术管控层面，利用隐私计算、区块链、加密认证等技术，搭建合规管控技术平台，实现对软件开发各环节的数据、技术、操作的实时监控与合规校验。

5.2 事前预防阶段的合规管控措施

事前预防阶段的合规管控聚焦于医疗 AI 软件开发的需求分析、技术选型、数据采集前期，通过前瞻性的规划与管控，从源头规避合规风险。首先，开展合规风险评估，结合软件的应用场景、技术方案、数据来源，梳理软件开发过程中可能存在的法律风险、行业规范风险、技术应用风险，形成风险评估报告，针对高风险点制定针对性的防范措施。其次，完善数据采集与使用的合规流程，明确数据采集的范围、方式、来源，对采集的医疗数据进行分级分类，针对敏感数据制定单独的采集与使用规范，提前完成数据主体的告知与同意流程，留存相关证明材料。再次，开展技术选型的合规审核，对选用的隐私计算技术、AI 技术进行合规性验证，确认技术方案符合法律、行业规范的要求，同时核查技术提供方的资质与能力，保障技术应用的合规性与稳定性。

5.3 事中管控阶段的合规管控措施

事中管控阶段的合规管控覆盖医疗 AI 软件开发的全流程，包括数据处理、模型开发、模型测试、产品部署等环节，通过实时监控、动态校验、及时整改的方式，保障各环节的合规运行。数据处理环节，利用合规管控技术平台对数据采集、清洗、标注、划分的全过程进行实时监控，对数据的传输、存储、使用进行加密与审计，确保数据处理符合分级分类保护的要求，同时对数据处理结果进行合规校验，避免违规处理数据的行为。模型开发环节，对模型的训练过程、参数聚合、迭代优化进行全程记录，保障模型开发的可追溯性，同时对 AI 模型的算法逻辑、决策机制进行合规审核，确保模型无算法歧视、算法黑箱等问题，契合行业伦理规范。模型测试环节，对测试数据的合规性、测试流程的规范性、测试结果的有效性进行全面审核，确保测试过程符合医疗 AI 软件的注册审查要求，测试结果能够真实反映模型的性能。产品部署环节，对部署环境、部署方式、数据对接进行合规校验，确保软件部署符合医疗机构的信息化规范与数据安全要求，同时完成软件的注册审批等相关手续，取得合法的市场准入资质。

5.4 事后追溯阶段的合规管控措施

事后追溯阶段的合规管控聚焦于医疗 AI 软件部署后的运行维护、问题处理、优化升级，通过建立完善的追溯机制，实现对合规问题的及时处置与全程追溯。首先，建立数据与技术的全生命周期追溯体系，利用区块链技术对软件开发各环节的原始数据、处理结果、模型参数、操作行为进行上链存证，实现数据与技术行为的不可篡改、可追溯，若发生数据泄露、合规违规等问题，能够快速定位问题源头，明确责任主体。其次，建立合规问题应急处理机制，制定数据泄露、模型异常、合规违规等问题的应急预案，一旦发现问题，立即启动应急处理流程，采取数据封存、系统关停、漏洞修复等措施，降低合规风险造成的损失，同时及时向相关监管部门报告，履行信息披露义务。

6 结论

本研究围绕基于隐私计算的医疗 AI 软件开发及合规性展开系统分析，明确了隐私计算与医疗 AI 软件开发的融合逻辑，设计了包含需求分析、数据处理、模型开发、部署运维的全流程开发方案，梳理了法律、行业规范、技术应用三个维度的合规核心要求，搭建了“事前预防、事中管控、事后追溯”的全流程合规管控体系。

参考文献

[1]莫琳芳，李喆，甘辉亮，等.全球视野下医疗人工智能中患者隐私和数据安全：焦点与策略[J].海军军医大学学报，2025，46（08）：989-999.

[2]裴新军.边缘计算 AI 应用的安全与隐私保护[D].中南大学，2024.

[3]王燕萍，金钢，王蓓蕾.医疗人工智能的法律问题分析与思考[J].卫生软科学，2024，38（02）：51-55.

作者简介：张跃华，出生年月：1987.9.10，男，汉族，籍贯：浙江金华，学历：本科，研究方向：人工智能、大数据；

张南极，出生年月：1992.6.26，男，汉族，籍贯：浙江金华，学历：大学本科，研究方向：软件设计、大数据；

赖俊朴，出生年月：2004.4.8，男，汉族，籍贯：浙江衢州，学历：大专，研究方向：信息化、人工智能