数字经济与管理
Digital Economy and Management

Vol. 3, No. 1 Mar. 2025
DOI: 10.12414/dem.250502

隐私计算技术在医疗数据共享中的应用边界

黄燕

（巴中职业技术学院　四川　巴中　636000）

摘　要　医疗数据共享在促进医疗健康领域的科研和服务提供方面扮演着重要角色，然而，数据安全和个人隐私保护问题一直是阻碍其广泛应用的主要难题。鉴于此，本论文探讨了隐私计算技术在医疗数据共享中的应用边界。我们首先介绍了隐私计算技术的概念以及主要的技术手段，如密码学、差分隐私、联邦学习等，并深入阐述了它们在医疗健康领域的具体应用。然后，我们分析了隐私计算技术在医疗数据保护中的优势和挑战，包括数据的安全性、数据的真实性、技术的复杂性等问题。接着，我们通过挖掘现有的医疗数据集和实例以及进行依赖隐私计算技术的模拟实验，确定了隐私计算技术在医疗数据共享中的应用边界。最后，我们发现，隐私计算技术对于保护医疗数据的安全具有巨大的潜力，但同时也存在一定的局限性，需要我们持续的研究和探索。整体而言，本研究有助于进一步理解隐私计算技术在医疗数据共享中的应用边界，并为未来的研究提供了有益的参考。

关键词　隐私计算技术；医疗数据共享；数据安全；差分隐私；联邦学习

文章编号　057-2025-0502

Application Boundaries of Privacy-Preserving Computation Technologies in Medical Data Sharing

Huang Yan

(BaZhong Vocational and Technical College, Bazhong 636000, China)

Abstract　Medical data sharing plays a pivotal role in advancing scientific research and service delivery within the healthcare sector. However, issues related to data security and personal privacy protection have been major obstacles hindering its widespread application. In light of this, this paper explores the application boundaries of privacy-preserving computation technologies in medical data sharing. We first introduce the concept of privacy-preserving computation technologies and their primary technical approaches, such as cryptography, differential privacy, federated learning, etc., and delve into their specific applications in the healthcare field. Subsequently, we analyze the advantages and challenges of privacy-preserving computation technologies in medical data protection, including issues related to data security, data authenticity, and technical complexity. By examining existing medical datasets and examples, as well as conducting simulation experiments relying on privacy-preserving computation technologies, we then determine the application boundaries of these technologies in medical data sharing. Finally, we find that while privacy-preserving computation technologies

收稿日期：2025-01-04　**录用日期**：2025-02-18

通讯作者：黄燕；**单位**：巴中职业技术学院　四川　巴中

hold significant potential for safeguarding the security of medical data, they also possess certain limitations that necessitate ongoing research and exploration. Overall, this study contributes to a deeper understanding of the application boundaries of privacy-preserving computation technologies in medical data sharing and provides valuable references for future research.

Keywords Privacy-preserving computation technologies; Medical data sharing; Data security; Differential privacy; Federated learning

在当前全球化和数字化迅速发展的背景下，医疗数据的共享已成为推动医疗科技进步和提升医疗服务质量的关键因素。医疗数据共享不仅可以帮助医疗机构提高治疗效率，还可以促进医疗研究，以便开发出更有效的治疗方案和药物。然而，与此同时，数据共享也伴随着显著的隐私和安全风险，个人敏感信息的泄露可能会导致严重的社会和个人问题。隐私计算技术作为一种新兴技术，为解决这一问题提供了可能。它通过加密算法和协议设计，在不泄露个人隐私信息的前提下，对数据进行加工和分析，保护用户数据在处理过程中的安全和隐私。主要技术手段包括密码学、差分隐私、联邦学习等，这些技术已在金融、通信等多个领域得到了广泛应用。尽管隐私计算技术在医疗数据共享方面展现出巨大的潜力，但其在实际应用中也遇到了诸多挑战。如技术实施的复杂性、高成本以及与现行法规的兼容问题等，这些问题都限制了其在医疗领域广泛应用的可能性。鉴于此，本论文旨在探讨隐私计算技术在医疗数据共享中的应用边界。通过对隐私计算技术在医疗健康领域的具体案例分析以及模拟实验，本研究将系统地评估隐私计算技术在保护医疗数据安全方面的优势与挑战，从而为该技术的进一步研究和优化提供理论和实践依据。

1 医疗数据共享的现状与挑战

1.1 医疗数据共享的重要性

医疗数据共享在医疗健康领域具有重要意义，其核心在于提升医疗服务效率、推动医学研究进步以及实现精准医疗目标 [1]。通过不同医疗机构的协作与数据共享，患者能够享受更为广泛且个性化的诊疗服务，诊断准确性和治疗成功率得以显著提高 [2]。大规模医疗数据的整合和分析能够为疾病的流行趋势预测、药物研发以及公共卫生政策制定提供重要依据，有助于实现医疗资源的优化配置。医疗数据共享能够促进人工智能技术在疾病诊断和治疗中的应用，为复杂病例提供可靠辅助决策依据。这种信息流动不仅关乎个体健康，也关系到整个社会的健康管理体系效率的提升和创新驱动。

1.2 医疗数据共享面临的难题

医疗数据共享在实践中面临多方面的难题。数据隐私和安全性始终是首要关注点，医疗数据包含敏感的个人健康信息，若被非法获取或滥用，将对个人及社会产生严重后果 [3]。数据标准化不足导致跨机构的数据整合困难，各医疗机构使用不同的数据格式或规范，增加了共享和交互的复杂性 [4]。法律和伦理约束限制了数据共享的范围，医疗数据的使用需严格遵守相关法律法规及保护患者权益的要求。技术成本较高及实施难度较大阻碍了先进技术在医疗数据共享中的广泛应用。这些难题共同制约了医疗数据共享的实际推进及其潜力发挥 [5]。

1.3 医疗数据安全保护的需求

医疗数据的安全保护至关重要，直接关系到个人隐私防护和医疗服务的可信度，其需求涵盖了数据加密、身份认证、访问控制等关键技术手段。

2 隐私计算技术概述

2.1 隐私计算技术的基本概念

隐私计算技术是一系列旨在保护数据隐私和安全的技术手段与方法。其基本概念包括通过对数据进行加密、匿名化和去标识化等处理，使数据在共享和分析过程中无泄露风险。隐私计算技术关注在保证数据隐私的确保数据的完整性和真实性。常用的隐私计算技术包括密码学、差分隐私以及联邦学习，这些技术通过数学和算法的方式实现数据保护。密码学技术主要依托加密算法保护数据的机密性；差分隐私通过添加噪声保证数据隐私；联邦学习则通过分布式机器学习方式避免数据集中存储带来的隐私风险。

2.2 主要的隐私计算技术手段

主要的隐私计算技术手段包括密码学、差分隐私和联邦学习等。密码学通过对数据进行加密，确保数据在传输和存储过程中的安全性和完整性。差分隐私则通过在数据中引入噪声，避免暴露个人信息，保持数据整体统计特性的准确性。联邦学习允许多个机构在不共享原始数据的前提下，共同训练机器学习模型，既能提高模型的准确度，又能有效保护数据隐私。这些技术在不同程度上解决了数据隐私和安全问题，为医疗数据共享提供了保障 [6]。

2.3 隐私计算技术的发展态势

隐私计算技术近年来在理论研究和实践应用方面取得了显著进展。密码学领域的发展推动了先进安全协议的设计，为隐私保护提供了更高效的算法支持 [7]。差分隐私的理论模型逐步完善，如噪声机制的优化增强了其应用场景的可行性。联邦学习技术从分布式架构和模型聚合角度不断迭代，适用于跨机构的协同数据分析需求 [8]。伴随人工智能、大数据和云计算的持续进步，隐私计算技术正向高精度、高适应性和广泛应用迈进，为敏感数据保护和价值挖掘带来新的可能 [9]。

3 隐私计算技术在医疗领域的应用

3.1 密码学在医疗数据安全中的应用

密码学在医疗数据安全中的应用是隐私计算技术的重要组成部分。通过使用加密算法，医疗数据能够在存储和传输过程中保持机密性，有效防止未经授权的访问。对称加密和非对称加密是主要的密码学技术，对称加密通过相同的密钥进行数据的加解密，而非对称加密则利用公钥和私钥进行数据保护。密码学技术还提供签名和验证功能，确保数据的真实性及其来源的可靠性。哈希函数也是用于数据完整性保护的重要工具，检测数据是否被恶意篡改。总的来说，密码学为保障医疗数据的安全性提供了坚实的基础 [10]。

3.2 差分隐私在医疗数据安全中的应用

差分隐私是一种用于确保数据共享时个人信息不被泄露的技术，通过在数据中添加噪声来保护个体隐私。差分隐私技术可以保证在统计分析过程中，原始数据不会被直接暴露，从而有效抵御重识别攻击。在医疗数据共享中，差分隐私可以应用于病患记录、药物使用情况等敏感数据的统计分析，确保个人隐私不被泄露，仍能提供高质量的数据分析结果 [11]。差分隐私的应用不仅提高了数据安全性，还促进了医疗研究和服务质量的提升。

3.3 联邦学习在医疗数据安全中的应用

联邦学习作为一种分布式机器学习技术，能够在多方之间实现数据不共享条件下的联合建模，在医疗数据安全中具有重要应用价值。该技术允许各数据持有方保留原始数据，仅交换模型参数，从而显著降低数据泄露风险。通过在医疗领域构建联邦学习框架，医疗机构间得以安全地

共享病患信息以进行联合分析，实现疾病预测与个性化诊疗，确保隐私数据不外泄。联邦学习在医疗数据共享应用中仍面临通信效率、异构数据处理以及模型性能等方面的挑战，需持续优化算法与实践策略以充分发挥其潜力。

4 隐私计算技术在医疗数据共享中的应用边界探索

4.1 隐私计算技术的优势和挑战

隐私计算技术在医疗数据共享中展现了诸多优势。通过密码学，可以有效地保护数据的完整性和保密性，减少数据在传输过程中被非法窃取的风险。差分隐私技术能够在统计分析过程中保护个人隐私，确保个体的数据无法被识别 [12]。联邦学习允许医疗机构在不共享患者数据的前提下进行联合建模，有助于保护数据隐私。这些技术也面临挑战。包括实现技术的复杂性高，资源消耗大，且对用户的专业技能要求较高。隐私算法的正确实施和优化仍需要不断的研究和实践。

4.2 确定隐私计算技术的应用边界

隐私计算技术在医疗数据共享中的应用边界主要体现在数据安全性和可用性间的平衡。在数据安全性方面，隐私计算技术能够有效保护数据不被未授权访问者获取，保障数据传输过程中的隐私 [13]。技术实现的复杂性和计算资源的要求会对实际应用产生制约 [14]。尤其在处理大数据集时，隐私计算技术可能导致计算效率降低，影响数据共享的及时性和质量 [15]。不同技术手段面对的具体应用场景和数据类型也各有优势和局限，需要根据具体需求和场景进行选择。这些因素共同决定了隐私计算技术在医疗数据共享中的应用边界。

4.3 针对隐私计算技术的应用策略

隐私计算技术在医疗数据共享中的应用策略包括加强多方合作、建立标准化的数据共享协议、完善数据治理机制、推广隐私保护措施的培训与教育，以及推动相关法律法规的制定。这些策略旨在提高数据安全性与可控性，促进技术的广泛应用与落地，保障医疗数据共享在隐私计算技术支撑下安全、可靠、高效地进行。有效的隐私计算策略不仅能提升医疗数据的保护水平，还能增强公众对医疗数据共享的信任与接受度。

5 隐私计算技术的前景与局限性

5.1 隐私计算技术对医疗数据安全的贡献

隐私计算技术在医疗数据安全领域发挥了重要作用，其核心在于通过技术手段确保敏感数据在使用、传输和分析过程中的隐私性与完整性。密码学方法使得医疗数据能够在加密状态下安全存储和共享，而差分隐私技术在数据分析中有效减少了个人信息泄漏的风险，保护了数据主体的隐私权。联邦学习突破了数据孤岛的限制，使多方参与的机器学习模型能够在本地数据不被直接共享的前提下协同训练。这些技术减少了恶意攻击和数据滥用的可能性，提升了医疗数据共享的效率和安全性，为医疗科研和服务创新提供了可靠的技术支持。这些贡献彰显了隐私计算技术在医疗领域应用中的潜力，为解决数据隐私保护问题提供了重要路径。

5.2 探讨隐私计算技术的局限性

隐私计算技术在医疗数据共享中的应用虽然展示了显著的潜力，但也面临一些局限性。技术复杂性增加了实施和维护的难度，高昂的成本限制了普及。法律和伦理问题在数据的跨境流通中易引发争议，隐私保护与数据利用之间的平衡也难以掌握。不同技术之间的兼容性问题也影响了其广泛应用。处理大规模数据时，计算效率和性能仍需提升。隐私计算技术的滥

用风险和潜在隐患不能忽视。

5.3 针对隐私计算技术未来的研究方向

未来研究应强化隐私计算技术与医疗数据共享需求的适配性，加强技术对多样性医疗场景的支持，优化算法效率以降低计算复杂度。应注重隐私计算技术在跨机构数据协作中的应用规范，提升数据安全性与真实性。在技术突破的需完善相关法律法规与伦理框架，确保隐私计算技术使用过程中的合规性。推动隐私计算技术向边缘计算与量子计算领域发展可能成为关键方向，以满足医疗数据处理的高效性与安全性要求。

6 结束语

本研究系统地分析了隐私计算技术在医疗数据共享中的应用以及遇到的挑战。通过深入探讨密码学、差分隐私和联邦学习等隐私计算技术，成功展示了它们在确保医疗数据保护中的独特优势与应用潜力。研究发现，尽管这些技术能显著提升数据共享过程中的安全性和隐私性，技术实施的复杂性与数据真实性依然是需要重点关注的问题。此外，本文通过实例分析和模拟实验确定了隐私计算技术的应用边界。尽管存在局限性，但这些先进技术对于促进医疗健康领域的发展仍具有不可忽视的积极意义。针对现有技术复杂性及数据安全的双重挑战，未来研究需要进一步优化技术方案和提高技术可操作性，同时也应探索新的隐私保护方法，以更好地服务于医疗数据共享。总之，此研究为理解隐私计算技术在医疗数据共享中应用的边界提供了有价值的视角，并为未来研究的方向和深入探讨奠定了坚实的基础。随着技术的不断进步和法规的相应改进，预期隐私计算技术将在医疗数据共享中发挥更加关键的作用，实现数据共享与隐私保护的更好平衡。

参考文献

[1] 徐语聪 . 隐私计算实现数据价值共享的关键技术 [J]. 数据 ,2021,(01):22-23.

[2] 胡奥婷 , 胡爱群 , 胡韵 , 李古月 , 韩金广 . 机器学习中差分隐私的数据共享及发布 : 技术、应用和挑战 [J]. 信息安全学报 ,2022,7(04):1-16.

[3] 郑谐维 . 隐私计算在政务数据共享中的应用 [J]. 上海信息化 ,2022,(04):17-21.

[4] 赵精武周瑞珏 . 隐私计算技术 : 数据流动与数据安全的协同保护规则构建 [J]. 信息通信技术与政策 ,2021,(07):53-58.

[5] 李月 , 张君 , 潘启娣 , 庄成诚 , 陶黎 . 隐私计算技术在海关大数据风控场景下的应用探索 [J]. 中国口岸科学技术 ,2023,(10).

[6] 魏晋 , 降惠 , 武丽娟 . 盲量子计算为核心的医疗隐私数据共享模型设计 [J]. 计算机时代 ,2023,(10):32-34.

[7] 冯云青 , 王梦鸽 . 基于隐私计算技术的数据生态合作应用 [J]. 信息技术与标准化 ,2023,(08):54-58.

[8] 王国赛 , 李艺 , 陈琨 , 时代 , 杨祖艳 . 隐私计算技术的金融应用思考 [J]. 金融发展研究 ,2022,(08):31-37.

[9] 杨晶 . 基于隐私计算技术的数据安全应用研究 [J]. 中国科技产业 ,2021,(10):61-63.

[10] 安鹏 , 张卓晖 , 喻波 . 基于微服务与隐私计算技术的数据安全共享服务平台 [J]. 信息安全研究 ,2022,8(10):1000-1007.

[11] 张雪明 . 应用隐私计算技术实现数据安全 [J]. 网络安全和信息化 ,2023,(01):3-6.

[12] 张铭杰 . 隐私计算技术赋能金融数据安全共享 [J]. 中国农村金融 ,2023,(04):97-98.

[13] 黄精武 . 基于差分隐私的联邦学习数据隐私安全技术 [J]. 通信技术 ,2022,55(12):1618-1625.

[14] 张丽萍 . 基于隐私计算技术的数据安全可信能力平台研究及应用 [J]. 电子测试 ,2022,36(23):137-139.

[15] 姚明 . 数据安全立法助推隐私计算技术的应用与创新 [J]. 国际品牌观察 ,2021,(26):38-39.