基于云计算的医疗数据共享平台隐私保护策略分析

王 暄[1] 侯 羿[2]
1. 中国人民解放军32701部队 北京 100071
2. 火箭军特色医学中心医学工程科 北京 100088

摘 要：在“健康中国2030”战略深入推进与数字医疗技术迅猛发展的双重驱动下，基于云计算的医疗数据共享平台已成为提升医疗服务效能、推动医学研究创新及优化公共卫生治理的核心基础设施。由于医疗数据承载着高度敏感的个人健康信息，其在云端集中存储与跨机构共享过程中面临严峻的隐私泄露风险。本文系统梳理了云计算环境下医疗数据共享平台的典型安全风险，包括数据泄露、未授权访问、身份关联攻击及合规性挑战；进而从技术、管理与法律三个维度构建协同联动的隐私保护策略体系。技术层面聚焦差分隐私、同态加密等前沿密码学与安全计算技术的应用；管理层面确立基于角色的访问控制、数据生命周期治理及安全审计制度；法律层面依据《中华人民共和国个人信息保护法》《中华人民共和国数据安全法》及国际相关法规，提出合规框架建议。

关键词：云计算；医疗数据共享；隐私保护；差分隐私；同态加密；数据安全

引言

随着全球医疗信息化进程加速，电子健康记录等海量医疗信息指数级增长态势，传统存储管理模式已难以满足跨区域诊疗、远程会诊、多中心联合科研以及分级诊疗协同等新型医疗需求。云计算凭借其弹性扩展与成本效益优势，已成为构建医疗数据共享平台的核心支撑，可实现跨机构、多主体的高效实时数据交换与协同分析，显著提升医疗资源配置效率与科研创新能力。然而，医疗数据具有高度敏感性，一旦泄露或滥用可能造成严重后果。云计算环境的特性进一步加剧了隐私保护的复杂性，云服务商管理疏漏、外部攻击、数据共享中的二次利用与关联分析等因素均可能引发隐私泄露问题。

1 云计算环境下医疗数据共享的隐私威胁分析

1.1 数据存储与传输风险

在 IaaS/PaaS/SaaS 等云服务模式下，医疗数据需上传至远程服务器。若传输通道未加密（如使用 HTTP 而非 HTTPS），数据易遭中间人攻击导致数据被截获；即便采用 TLS 加密，密钥管理不当或协议漏洞（如 Heartbleed）仍可能导致数据泄露。存储环节中，若云平台未实施强加密或密钥由服务商单方控制，一旦发生内部人员越权访问或外部入侵，原始数据将面临直接暴露风险。

1.2 多租户环境下的侧信道攻击

云平台通常采用虚拟化技术实现计算资源的共享分配，多个租户的虚拟机可能运行在同一物理服务器上。恶意租户可通过监控 CPU 缓存命中率、内存带宽占用、网络流量变化等侧信道信息，推断邻近虚拟机中其他用户的医疗数据操作行为，甚至重构部分敏感医疗信息。此类攻击具有极强的隐蔽性，传统防火墙、入侵检测系统等安全防护手段难以有效识别与防御。

1.3 身份重识别与关联攻击

医疗数据通常包含诊断记录、用药史、实验室检测结果等准标识符信息。攻击者若掌握部分外部公开数据（如社交媒体信息、人口统计数据库），可通过链接攻击将将匿名化后的医疗记录与特定个体关联[1]。例如，Sweeney 的研究证实，仅凭邮政编码、出生日期和性别这三项基础信息，即可识别出美国 87% 人口的医疗记录，匿名化处理难以有效抵御此类关联攻击。

1.4 共享过程中的权限失控

在跨机构数据共享场景中，数据提供方难以对数据接收方的后续使用行为进行有效管控。部分接收方可能将医疗数据用于未经授权的用途（如商业营销、第三方合作），或擅自将数据再次共享给其他主体，形成“数据链式泄露”。传统的静态访问控制模型（如 ACL 访问控制列表）难以适应动态变化的跨机构协作需求，无法实现权限的精细化、动态化管理。

1.5 法律与合规风险

《中华人民共和国个人信息保护法》明确将医疗健康信息列为敏感个人信息，要求采取严格的保护措施；《中华人民共和国数据安全法》则强调对重要数据的分类分级保护与出境安全评估。国际层面，欧盟 GDPR 对跨境数据传输设定了严格标准（如标准合同条款 SCCs），美国 HIPAA 法案也对医疗数据保护提出了明确要求。若医疗云平台部署在境外服务器，或采用跨国云

服务提供商的服务，极易触碰各国数据保护法律红线，引发高额罚款或业务中断。

2 隐私保护策略体系构建

针对云计算环境下医疗数据共享面临的多层次、多维度隐私威胁，本文提出“技术—管理—法律”三层协同的隐私保护策略框架，通过硬性技术防护、柔性管理制度与刚性法律约束的有机融合，构建全方位、立体化的纵深防御体系。

2.1 技术防护层：密码学与安全计算

2.1.1 差分隐私

差分隐私作为一种形式化的隐私保护定义，通过向统计查询结果注入可控的随机噪声，确保任何单个个体的存在与否对输出分布的影响在可接受范围内，从而在理论上杜绝了重识别的可能性。该技术适用于疾病发病率统计、平均住院天数分析等聚合数据发布场景，也可在联邦学习中对模型梯度更新进行噪声扰动，保护参与方的本地医疗数据隐私。尽管噪声注入会在一定程度上降低数据精度，但通过合理设定隐私预算（ε值）并结合自适应调整机制，可在隐私保护强度与数据应用效用之间实现动态平衡。

2.1.2 同态加密

同态加密技术突破了传统加密技术“解密后才能计算”的限制，允许在密文状态下直接执行加法、乘法等计算操作，解密后得到的结果与对明文数据计算的结果完全一致。全同态加密技术虽面临计算开销较大的问题，但在基因组数据比对、高精度医学建模等高敏感场景中具有不可替代的价值；而部分同态加密方案（如Paillier）则能高效支持求和、计数等常见聚合操作，适合用于医保费用结算、区域健康指标统计等任务[2]。

2.1.3 属性基加密

属性基加密（ABE）将访问控制逻辑内嵌于加密机制之中，打破了传统公钥加密“一对一”的密钥分发模式。该技术将用户权限抽象为属性集合（如“医院等级 = 三甲”“科室 = 肿瘤科”“角色 = 研究员”），数据加密时绑定特定的访问策略（以布尔表达式形式呈现），仅当用户的属性集合满足访问策略时，才能成功解密数据。这种机制天然支持细粒度、动态化的权限管理，能够精准适配多机构联合研究、分级诊疗协作等复杂场景，有效防止权限过度授予或滥用引发的隐私风险。

2.1.4 可信执行环境

可信执行环境（TEE）从硬件层面构建了安全隔离的执行空间，以 Intel SGX 为代表的 TEE 技术在 CPU 内部创建加密“飞地”（Enclave），确保其中运行的代码和数据即使在操作系统或虚拟机监控器被攻陷的情况下，仍能保持机密性与完整性。医疗数据分析程序可在 TEE 内安全加载运行，原始医疗数据仅在飞地内部进行解密处理，最终仅输出经过验证的计算结果。该技术能够有效抵御侧信道攻击与内部威胁，为高价值医疗数据计算任务提供可信执行环境。当然，TEE 并非绝对安全，其远程证明机制的可靠性及已知漏洞（如 Foreshadow 漏洞）仍需持续优化与加固。

2.1.5 零知识证明

零知识证明（ZKP）允许证明方在不透露任何额外信息的前提下，向验证方证明某个陈述的真实性。在医疗身份认证、权限申请等场景中，患者可利用ZKP向系统证明自己满足“年龄 ≥ 18 岁且患有糖尿病”等特定条件，无需暴露具体出生日期或诊断编码[3]。这种“证明而不泄露”的特性，充分体现了隐私保护的“最小必要”原则，为构建以用户为中心的隐私增强型医疗服务提供了技术支撑。

2.1.6 管理机制层：制度与流程保障

2.1.7 基于角色的动态访问控制

摒弃传统静态、粗粒度的授权模式，构建融合角色（Role）与属性（Attribute）的混合访问控制模型。该模型不仅依据用户所属组织、岗位角色分配基础权限，还结合实时上下文信息（如登录地点、设备安全状态、操作时间、业务场景）动态调整访问权限等级，并辅以多因素认证（MFA）、分级审批工作流等机制，确保每一次数据访问操作都经过严格验证与授权，实现“权限最小化、操作可追溯”。

2.1.8 数据生命周期治理

建立贯穿数据采集、存储、使用、传输、销毁全流程的生命周期治理机制。在采集阶段，严格遵循“最小必要”原则，明确告知患者数据收集目的、使用范围、保存期限等信息，获取患者书面同意；在存储阶段，对医疗数据进行分级分类管理（如将核心电子病历、基因组数据列为高敏感数据，系统日志列为普通数据），针对不同级别数据施加差异化的加密、备份与访问控制策略；在使用阶段，强制记录所有数据访问、查询、修改、导出等操作，形成不可篡改的操作日志。

2.1.9 安全审计与应急响应

构建健全的安全审计与应急响应机制。部署安全信息与事件管理（SIEM）系统，对数据访问行为进行实时监控，对非工作时间高频下载、跨地域异常访问等行为实时告警阻断。定期开展渗透测试、漏洞扫描与隐私影响评估（PIA），主动发现风险[4]。制定详尽的数据泄

露应急预案，明确风险评估、事件上报、通知受影响个体、启动损害控制措施等关键流程，要求在 72 小时内完成向监管机构的报告，最大限度降低事件负面影响。

2.1.10 法律合规层：制度衔接与跨境协调

2.1.11 国内法规遵从

严格遵守《中华人民共和国个人信息保护法》对敏感个人信息处理的特殊规定，包括但不限于：取得个人单独书面同意、开展事前个人信息保护影响评估、公开透明的数据处理规则、采取加密、去标识化等安全保护措施。同时，满足《中华人民共和国数据安全法》对重要数据分类分级保护的要求，依据《网络安全等级保护基本要求》完成三级及以上等级保护测评，确保平台安全防护水平符合法定要求。

2.1.12 跨境数据流动合规

针对跨境数据流动场景，建立严格的合规管理机制。优先选择境内云服务商，将医疗数据存储在我国司法管辖范围内，保障数据主权。确因国际合作研究等正当理由需向境外提供医疗数据，必须依法通过国家网信部门组织的数据出境安全评估，或采用经批准的标准合同条款（SCCs）等合法路径。在数据处理协议中明确境外接收方的数据保护义务、数据使用范围、违约责任及接受我国监管机构监督的承诺，确保患者隐私权益在全球范围内得到同等保护。

3 挑战与未来展望

本文提出的策略体系在实际部署中仍面临多重挑战：其一，性能与成本平衡难题，同态加密、可信执行环境等前沿技术目前存在计算开销大、部署成本高的问题，难以直接应用于高并发、低延迟的实时临床诊疗场景，亟需通过算法优化（如近似同态加密方案）、专用硬件加速等方式提升性能、降低成本。其二，隐私保护与数据效用的内在张力，尤其是在罕见病研究、精准医疗建模等对数据精度要求极高的场景中，差分隐私等技术注入的噪声可能掩盖关键数据信号，未来需研发更智能的隐私预算分配机制、高质量合成数据生成技术，在强化隐私保护的同时保障数据应用价值。其三，行业标准缺失导致的互操作性问题，当前各医疗云平台的数据格式、接口协议、安全规范存在差异，阻碍了医疗数据的跨平台高效流通，亟需政府部门与行业协会牵头制定统一的行业标准与技术规范。其四，信任体系构建问题，技术与制度难以完全替代信任，需建立包含患者代表、医疗机构、监管部门、技术专家在内的数据治理委员会，通过透明化治理机制增强社会监督与伦理约束。

展望未来，隐私增强机器学习（PEML）将成为重要方向，通过融合联邦学习、安全多方计算与差分隐私，构建端到端隐私保护 AI 流水线；区块链技术可在访问控制与审计溯源中发挥作用，利用智能合约实现数据使用协议自动执行。

4 结语

云计算为医疗数据共享开辟了广阔前景，隐私保护是其可持续发展的基石。本文系统剖析了医疗云平台的多重隐私威胁，构建并论证了“技术—管理—法律”三位一体的综合防护策略。研究表明，单一手段难以应对复杂风险，需通过密码学创新、精细化管理制度与严格法律合规的深度融合，构建纵深防御体系。未来，随着技术演进与法规完善，医疗数据将在安全可信环境中释放更大社会价值，助力精准医疗与公共卫生事业高质量发展。

参考文献

[1]刘楚菲,刘宇辰.基于云计算的医疗数据共享平台构建[J].长江信息通信,2023,36(05):121-123.

[2]孙宗锟.面向智慧医疗云平台数据使用的隐私保护研究[D].山东科技大学,2020.

[3]程德生,万晶,宋国彩,等.中医药大数据云服务平台的医疗数据安全隐私保护设计[J].网络安全技术与应用,2021,(02):122-124.

[4]徐秋亮,隐私保护的医疗数据融合应用公共服务平台.山东省,普联软件股份有限公司,2021-08-25.