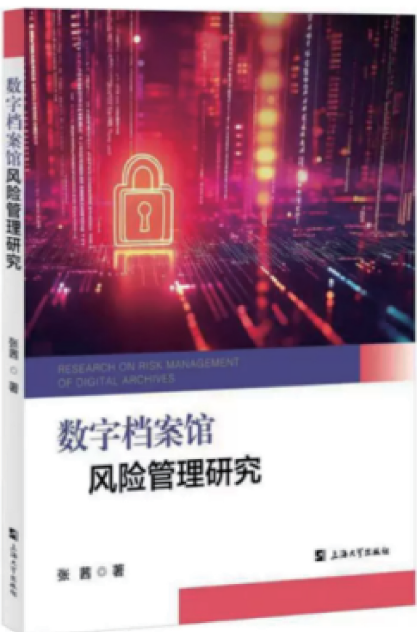
医疗数字档案管理风险与应对

——评《数字档案馆风险管理研究》

医疗数字档案存着患者个人信息、影像和病史等关键隐私数据信息，一旦泄露，会对患者个人权利造成伤害，医疗机构亦会背负法律责任。因此，医疗机构须做好医疗数字档案的风险管理，保证数据真实、不泄密，才能维持行业健康可持续发展，保护患者和医院的合法权益。

《数字档案馆风险管理研究》一书立足数字化转型时代背景，以风险管理的全生命周期理论为指导，构建了“风险识别-风险评估-智能应对”的安全管理模式。全书共9章，第1章—第5章为理论基础，基于云计算、大数据、区块链，以及人工智能等技术，探索新型风险形态，并结合开放档案信息系统模型与文件连续体模型，界定了数字档案馆风险的定义、特征及分类标准，并在此基础上剖析了从风险识别、分析到评价的全流程风险管控体系，且特别强调了自然灾害、技术故障、人为泄密及法律合规等多维风险源。第6章—第9章聚焦实战与前沿，基于对美国等国家的数字档案馆风险管理的经验与模式，提出行政、技术、资源3层面的立体化应对方略，亦创新性引入知识图谱与区块链技术，推动了数字档案馆智能化安全管理相关研究的深入。



书名：数字档案馆风险管理研究
作者：张茜
出版社：上海大学出版社
ISBN：9787567154971
出版时间：2025年11月
定价：88元

该书作者指出，当下的医疗数字档案所面临的风险已不局限于病毒攻击，而是面临有组织、有预谋的多维攻击。受制于业务方向等因素影响，医疗机构数字档案建设工作相对滞后，整体管理水平不高。加上部分医疗机构的安全意识不强，且不懂专业的数据信息安全预防知识技巧，因此，在数据访问安全权限设置方面不够严谨，甚至会给一些实习生、规培生或外包运维工作人员较高的数据查询权限，由此会留下较大的安全隐患。一旦出现安全问题，则整个医院的数据信息都可能会被别有用心的灰产机构或个人获取，从而造成严重的医疗数据信息泄漏事故，带来无法预料的损失。基于此，医院档案管理部门必须摒弃“内网即安全”的固有思维，全面转向“零信任”架构，这意味着“永不信任，始终验证”。在此安全架构下，即便是院长在内的人员网访问档案，也必须经过多因素认证和生物特征识别。与此同时，医院有必要引入区块链存证技术。传统的日志审计可被黑客抹除痕迹，但区块链的不可篡改性让每一次查询、每一次下载都留下永恒的“数字指纹”。配合防扩散水印技术，一旦截图流出，能瞬间追溯到具体的操作员、设备甚至时间点，从而在出事之后迅速锁定风险点。

笔者认为，数字化不仅是载体的变化，更是内容的重构。现实痛点在于，一些医疗数据虽然已上线，但变成了无法利用的“死数据”甚至“毒数据”。为利用数据，医疗机构会使用人工智能（Artificial Intelligence，AI）技术进行数据挖掘，然而这同样也会带来难以预测的风险。在调试光学字符识别（Optical Character Recognition，OCR）和自然语言处理模型时，若不加干预，AI生成的技术方案可能会存在错误，这种错误混入临床决策系统，可能导致误诊。更棘手的问题是电子档案的“原始性”可能丧失——电子文件极易被无痕篡改，且难以像纸质档案那样通过笔迹鉴定真伪。当发生医疗纠纷时，如果无法证明电子病历未被修改，医院将面临巨额赔偿。同时，由于AI技术处于发展初期，各厂商系统接口标准不一，形成了无数个数据孤岛，档案数据无法在科研、临床、管理间自由流动，所谓的“大数据”成了一盘散沙。面对这种情况，技术人员不能只做“搬运工”，必须成为“数据炼金师”。首先，要建立全流程的数据清洗与质控中台，在档案数字化入口端，利用高精度OCR和医学知识图谱自动校验数据，如系统自动识别“男性患者出现子宫肌瘤”这类逻辑错误并报警，而非照单全收。其次，必须死守“脱敏与合规”底线，在利用AI进行科研挖掘前，必须通过差分隐私技术对数据进行不可逆脱敏，确保“数据可用不可见”，对于涉及科研成果、重大传染病的机密档案，要采用联邦学习架构，让数据不出域即可完成模型训练。最后，统一标准打破孤岛，医疗主管部门推动建立全院级甚至区域级的统一元数据标准，强制要求所有业务系统按此规范存储，利用AI知识图谱技术，将碎片化的病历、影像、检验报告关联成一张动态的“患者全景图”。

总之，医疗数字档案风险管理的关键在于重构安全逻辑与治理思维，既要用最严苛的技术手段锁死风险的“后门”，亦要用最智能的算法预防风险，构建坚实的安全防线。

（孙娆/连云港市第一人民医院干部保健诊疗中心/副研究馆员）