智慧医院数字化信息安全治理策略
——评《智慧医院信息安全治理体系》

书名:智慧医院信息安全治理体系
编者:张武军
出版社:中山大学出版社
ISBN:9787306075079
出版时间:2022年9月
定价:78元

智慧医院通过物联网、大数据与人工智能等多重技术重构诊疗流程,但其开放化、集约化的信息系统架构正面临数据泄露、系统漏洞与隐私侵犯等多重风险。基于此,可构建多主体协同的治理机制,平衡技术创新与风险管控,为医疗数字化高质量发展提供实践路径。

《智慧医院信息安全治理体系》一书以医院信息化演进为逻辑起点,系统梳理了从基础系统建设到数字化转型的实践路径,特别强调5G、人工智能、区块链等新兴信息技术与医疗场景的深度耦合,揭示了智慧医疗对实时数据交互、精准诊疗支持、远程服务延伸的技术需求。在治理体系构建层面,该书突破传统技术导向的局限,创新性地提出"四维一体"安全架构:技术体系聚焦IaaS至SaaS层全栈防护,管理体系强化制度规范与人员能力建设,运营体系注重动态监测与持续改进,应急体系则构建了覆盖预案、响应、恢复的全周期机制。通过理论模型构建与典型案例分析,为医疗机构在数字化转型中平衡技术创新与风险管控提供了系统解决方案。

编者指出,智慧医院信息安全治理实践,可根据实际情况建立覆盖数据全生命周期的闭环管理体系,优化组织结构,理清权责。顶层可设立数据安全治理委员会,由医院院长、主管副院长、信息部门负责人及临床专家组成,负责制定全局性安全策略并审批重大决策;中层由专职数据安全官担任主管,统筹技术实施与部门协同;基层主要负责落实,具体可组建跨职能安全运营团队,涵盖IT工程师、合规专员及临床代表,确保业务需求与安全控制的平衡。技术防护层面可采用分层解耦、纵深防御的架构设计,分多个层级进行管理:基础层可设计数据分类分级机制,并电子病历、影像数据等实施三级分类保护,并运用形式化验证技术确保标签准确性;传输层部署数智化算法加密通道,结合量子密钥分发技术应对未来计算威胁;存储层构建混合云灾备体系,本地部署全闪存阵列保障热数据实时访问,私有云存储温数据,公有云存储冷数据,通过纠删码技术将存储开销降低40%;应用层实施动态访问控制,基于属性加密技术实现细粒度权限管理,结合零信任架构持续验证用户身份与设备状态。管理流程创新体现在3个维度:①建立双态IT管理模式,稳态系统遵循信息技术基础设施库框架强化变更管理,敏态系统采用开发安全运维一体化实现安全左移;②构建自动化合规引擎,集成《个人信息保护法》《医疗数据安全分类分级指南》等28项法规要求,通过自然语言处理、技术自动扫描制度文档与系统配置;③创建安全能力成熟度评估模型,参照美国国家标准与技术研究院网络安全框架设置137项控制指标,每季度开展差距分析并生成改进路线图。

笔者认为,面对高级持续性威胁与医疗物联网设备带来的新型风险,智慧医院需构建"预测-防御-检测-响应"四位一体的智能防御体系。在威胁预测层面,部署医疗专用威胁情报平台,通过联邦学习技术聚合数百家三甲医院的安全日志,运用图神经网络构建攻击者画像库,实现未知威胁的提前72 h预警。结合医院业务特性定制检测规则,如对"医学影像存档与通信系统"的医学数字成像和通信协议进行深度包检测,识别异常影像调取行为。防御体系构建强调"软件定义安全"理念。网络层采用意图驱动网络技术,通过中央控制器统一编排安全策略,实现东西向流量微隔离。终端安全引入扩展检测响应方案,整合终端检测与响应、云访问安全代理、网络即服务等多源数据,利用强化学习算法优化检测模型,将勒索软件识别率提升至99.2%。计算环境部署可信执行环境,在中央处理器层隔离敏感操作,确保基因测序、人工智能诊断等计算过程的数据机密性。在威胁治理方面,建立"平战结合"的应急响应机制。日常运营中通过自动化渗透测试持续验证防御有效性,运用模糊测试技术发现医疗设备固件漏洞。危机发生时,启动预设的剧本式响应流程,结合数字孪生技术模拟攻击扩散路径,指导物理隔离与系统回滚操作。事后治理环节,采用区块链存证技术固化攻击证据链,通过因果推理引擎分析事件根因,自动生成改进建议并更新安全知识库。

总之,智慧医院信息安全治理需持续融合技术创新与管理革新,通过多维度防护体系筑牢数字医疗安全屏障,以法治为基、技术为翼、管理为魂,共绘健康中国数字医疗新篇章。

(袁文博/常州市肿瘤医院/工程师)