



医共体信息化建设， 这几个问题必须解决

◎米易县人民医院 郑建军

医共体信息化建设，是提升医疗资源共享效率、优化医疗服务水平、强化医疗管理效能的关键举措。然而，在实际推进过程中，诸多挑战如同一座座大山横亘在前。本文将带您深入了解医共体信息化建设亟需解决的问题以及相应的解决办法。

数据互通：破除“语言壁垒”

医共体信息化建设首要难题是实现不同医疗机构数据互通互认，涵盖电子病历等。但各单位系统、数据格式等各异，如不同语言，致数据互通困难。

要解决医共体数据互通互认难题，统一数据标准、搭建数据交换平台、强化信息安全保障是关键。统一数据标准，就像为不同语言找到通用“翻译规则”，病历编码、疾病诊断编码等有了统一规范，各医疗机构数据才能无缝共享。构建集中数据交换平台，如同打造“数据枢纽”，汇聚各机构数据，实现顺畅流转共享。此外，数据互通过程中信息安全至关重要，通过数据加密、身份验证等建立安全互联网络，为数据传输加上“安全锁”，保障患者隐私，防止数据泄露。

系统兼容：摆脱“设备枷锁”

医共体内各级医疗机构的硬件和软件设备良莠不齐，部分单位还在使用老旧系统，其兼容性和稳定性较差，这无疑给信息化建设和数据共享套上了“枷锁”。

为打破这一困境，可采取硬件升级支持、建设云平台以及加强技术支持等措施。为基层单位提供硬件升级和维护支持，就像为老旧的

“汽车”更换新零件，使其硬件设备能与上级医疗机构的信息化系统兼容。建立一个云平台，将所有数据和系统功能迁移到云端，如同把物品从狭小的仓库搬到宽敞的“云端仓库”，减少对本地硬件的依赖。设立信息技术支持团队，提供7x24小时的技术支持，就像为各医疗机构配备“专属医生”，随时解决在使用信息化系统中遇到的兼容性和稳定性问题。

信息安全：筑牢“隐私防线”

随着医共体内部数据共享的深入，信息安全与隐私保护问题日益严峻。患者的健康数据及个人隐私一旦泄露，后果不堪设想。

解决医共体信息安全与隐私保护问题，需多管齐下。制定严格隐私保护政策，为数据使用划定“红线”，明确数据访问权限与使用范围，让各级人员只能获取工作所需数据。采用高强度数据加密和多重身份验证机制，给数据传输穿上“防弹衣”，保障传输安全。同时，搭建数据安全防护系统，实时监控拦截异常数据访问和外部入侵，通过设置防火墙、防病毒软件等安全措施，为数据筑起“铜墙铁壁”，实现数据全方位保护，让患者信息无虞。

人才资金：破解“资源困局”

医共体信息化建设需大量资金与人才，可基层医疗单位却资金短缺、人才匮乏。高昂的软硬件投入及人才维护成本，令其难以支撑信息化建设长期推进。

为破解基层医共体信息化建设资金与人才难题，可从3方面发力。一是争取政府及医疗管理部门支持，设立专项资金，优先投向基层信息化建设，宛如“及时雨”，缓解基层资金压力。二是引入社会资本，与第三方信息技术公司合作共建共维信息系统，如同引入“合伙人”，减轻基层资金负担。三是制定技术培训计划，通过内部培养与外部引进提升基层技术人员水平，并搭建远程支持和在线帮助平台，让基层人员快速获技术支持，为基层培育“技术骨干”，解决人才困境。

系统升级：应对“技术迭代”

医共体的信息系统在使用过程中需要不断进行维护和升级，以应对技术的快速迭代。

要解决这一问题，需制定系统的定期升级计划，及时引入最新的技术，保证系统的功能和性能处于最佳状态。在医共体内设立专门的维护团队，如同为系统配备“专属管家”，保证系统的稳定运行。采用模块化的系统架构，就像搭建“积木”，减少升级时的影响和成本，使系统升级更加灵活高效。

总之，医共体的信息化建设是一场攻坚战，需要攻克数据互通互认、系统兼容性和稳定性、信息安全与隐私保护、资金和技术人才短缺以及系统维护和持续升级等诸多难题。只有构建高效、安全、便捷的信息化系统，才能更好地服务群众，让优质医疗资源惠及更多人。☺