

Research on the Innovative Application of Next-Generation Communication Technologies in Modern Hospital Information Management

新一代通信技术在现代医院信息化管理中的
创新应用研究

伊拉特 著



**International
Union of Scientific and
Technological Scholars**

CIP INFORMATION

Title: Research on the Innovative Application of Next-Generation Communication Technologies in Modern Hospital Information Management

题目：新一代通信技术在现代医院信息化管理中的创新应用研究

Author: Late Yi

作者：伊拉特

ISBN: 979-8-90040-278-9

Publisher: CYPEDIA INTERNATIONAL UNION OF SCIENTIFIC AND
TECHNOLOGICAL SCHOLARS

Price: \$60.00

定价：60 美金



**International
Union of Scientific and
Technological Scholars**

**Research on the Innovative Application of Next-Generation Communication
Technologies in Modern Hospital Information Management
新一代通信技术在现代医院信息化管理中的创新应用研究**

Address: 100 N Howard St Ste R, Spokane, Wa, 99201. United States

Tel: +888-754-5177

Email: contact@cypedia.net

Format: 170mmx240mm 1/16 Sheets: 15.75

Word Counts: 210.000

Edition: First edition in July 2026

Printing: First printing in July 2026

**CYPEDIA INTERNATIONAL UNION OF SCIENTIFIC AND TECHNOLOGICAL
SCHOLARS**

非开放获取·电子版请联络出版社购买·版权归出版社所有·侵权必究

Not Open Access. For the electronic version, please contact the publisher for purchase. The copyright belongs to the publisher.
Infringement will be prosecuted.

PREFACE

前言

进入数字经济时代，以 5G-A、6G 为代表的新一代通信技术正以前所未有的速度与力度重塑各行业发展格局，医疗健康领域作为关乎民生福祉的核心领域，自然成为技术革新的重要阵地。与此同时，健康中国战略的深入推进与人民群众日益增长的多元化医疗需求，对现代化医院的管理效能与服务质量提出了更高要求。传统医院管理模式下的资源调度低效、服务流程繁琐、数据壁垒森严等问题愈发凸显，亟需借助新一代通信技术的东风，推动医院信息化管理实现系统性、深层次的创新变革。在此背景下，系统研究新一代通信技术在现代化医院信息化管理中的创新应用，探索技术融合赋能医院高质量发展的路径与方法，具有重要的理论价值与现实意义。

新一代通信技术凭借其高速率、低时延、广连接、高可靠的核心特性，为医院信息化管理突破传统瓶颈提供了强大的技术支撑。从 5G 技术实现远程会诊、智能护理的初步落地，到 5G-A 技术在超高清影像传输、精准导航定位等场景的深化应用，再到 6G 技术空天地一体化覆盖、通感算一体化等特性带来的全域协同医疗新可能，通信技术的每一次迭代都为医院信息化管理注入了新的活力。然而，技术的应用并非一蹴而就，新一代通信技术在与医院信息化管理融合的过程中，既面临着技术适配、数据治理、人才支撑等现实挑战，也需要政策引导与标准规范的有力保障。如何破解这些难题，充分释放技术红利，构建“智能、高效、协同、安全”的现代化医院信息化管理体系，成为当前医疗健康领域与信息技术领域共同关注的重要课题。

基于上述研究背景与现实需求，本书聚焦新一代通信技术与现代化医院信息化管理的深度融合命题，构建了“背景 - 保障 - 应用 - 挑战 - 对策”的完整研究框架。全书共分为六个核心章节：第一章立足数字中国与健康中国战略背景，阐述新一代通信技术发展态势及其对医院信息化管理的变革性影

响，明确本书的研究意义、研究思路与研究方法；第二章系统梳理新一代通信技术医疗应用的政策支持体系，从国家顶层规划、部门协同推进、地方精准落地三个维度，解析政策如何为技术应用保驾护航；第三章深入探讨行业标准化建设现状，涵盖基础通用标准、细分领域专用标准、数据安全与隐私保护标准，揭示标准规范在技术规模化应用中的核心作用；第四章是本书的核心内容之一，详细剖析新一代通信技术在医院信息化管理中的五大创新应用场景，包括智能化资源调度与管理、精准化成本管控与优化、全流程智能化服务管理、协同化科研与智能化教学管理、全方位安全管理与风险防控，结合具体应用模式展现技术赋能成效；第五章直面技术应用实践中的现实挑战，从技术适配、数据治理、人才短缺、资金压力、管理机制五个方面进行深度剖析；第六章针对性地提出解决方案，构建“技术 - 数据 - 人才 - 资金 - 机制”协同发展的全方位对策体系，为技术与医院信息化管理的深度融合提供实操路径。

在撰写过程中，本书兼顾理论深度与实践价值，注重政策解读与案例分析的结合、技术原理与应用场景的衔接。一方面，系统梳理相关政策文件与行业标准，深入剖析新一代通信技术的核心特性与应用逻辑，构建起较为完善的理论分析框架；另一方面，借鉴国内外医院信息化管理的创新实践经验，通过具体案例解析技术应用的痛点、难点与突破点，提升研究成果的可操作性与指导性。本书期望能够为医院管理从业者提供技术应用的实践指引，为医疗信息化技术研发人员明确技术创新的方向，为卫生健康领域政策制定者提供决策参考，也为相关专业高校师生搭建理论学习与实践探索的桥梁。

限于作者水平，书中难免存在疏漏及不妥之处，敬请读者批评指正。

作 者

CONTENTS

目录

第一章 新一代通信技术在现代医院信息化管理中的概述	1
第一节 研究背景与意义	1
第二节 新一代通信技术的核心特征与演进趋势	4
第三节 现代医院信息化管理的现存格局与核心挑战	8
第四节 通信技术与医院管理深度融合的创新价值与应用逻辑	12
第二章 5G 技术在医院信息化管理中的深度应用研究	17
第一节 5G 技术特点及其医疗场景适配性分析	17
第二节 5G 在远程精准诊疗中的创新应用	20
第三节 5G 支持下的医疗设备泛在互联与高可靠数据传输	24
第四节 5G 网络在突发公共卫生事件应急管理中的应用实践	27
第三章 物联网技术在医院信息化管理中的应用研究	33
第一节 物联网技术架构与医疗应用基础	33
第二节 智能医疗设备全生命周期管理与物资溯源闭环管理	37
第三节 物联网赋能的多维度患者监护与院内外健康协同管理	42
第四节 物联网在医院环境智能监控与预警中的应用	46
第四章 云计算与云原生技术在医院信息化管理中的应用研究	51
第一节 云计算服务模式与医疗信息化架构适配	51
第二节 电子病历与健康档案的云原生存储及跨院区共享平台构建	55
第三节 云计算支撑的医疗大数据挖掘与临床决策分析应用	60
第四节 云原生技术在智慧医疗场景应用效果评估	64

第五章 人工智能与新一代通信技术融合应用研究	69
第一节 AI 与通信技术（5G/ 边缘计算）融合的医疗技术基础与架构	69
第二节 智能诊断辅助与通信系统集成	72
第三节 基于人工智能 + 通信融合的医疗资源智能分配与调度	77
第四节 智能医患交互与通信体验场景优化	82
第六章 区块链技术在医疗信息安全管理中的创新应用研究	89
第一节 区块链原理与医疗数据安全需求匹配	89
第二节 基于区块链的医疗数据可信共享与隐私保护机制	92
第三节 区块链在药品全生命周期溯源与医疗供应链管理中的应用	97
第四节 智能合约在医疗结算中的应用实践	101
第七章 边缘计算与算力网络在医院信息化管理中的应用研究	105
第一节 边缘计算架构与医疗高实时性应用场景	105
第二节 边缘计算支撑的医疗实时数据处理与低延迟医疗服务	109
第三节 边缘计算赋能的移动医疗设备本地算力增强	113
第四节 边缘与云协同算力网络在医院多院区一体化业务中的应用模式 ..	117
第八章 新一代通信技术在医院管理流程优化中的应用	121
第一节 基于“通信 +”的全闭环就诊流程再造	121
第二节 通信技术支撑的多院区业务协同与信息互通	124
第三节 基于新一代通信技术的医院后勤智慧能力改造	128
第四节 通信技术驱动的医疗质量管理与动态监督体系创新	132
第九章 医院信息化安全与通信安全管理体系建设	137
第一节 新一代通信技术环境下医疗信息系统安全风险分析	137
第二节 医疗通信网络的安全防护策略	153
第三节 数据隐私保护与合规管理	171
第四节 医院信息化安全应急响应与灾备恢复机制	191

第十章 新一代通信技术引领的现代医院信息化发展趋势与展望 211

 第一节 6G 通信技术在医疗领域的应用前景 211

 第二节 新一代通信技术驱动的智慧医院建设的发展方向 218

 第三节 新一代通信技术应用的政策支持与行业标准化建设 225

 第四节 新一代通信技术在医院信息化管理中的创新应用面临的挑战与对策
..... 231

参考文献 241

第一章 新一代通信技术在现代医院 信息化管理中的概述

第一节 研究背景与意义

一、研究背景

（一）医疗行业数字化转型的必然诉求

随着我国医疗卫生事业的快速发展，现代医院的服务模式与管理体制正经历深刻变革，数字化、智能化已成为提升医疗服务质量与管理效能的核心方向。当前，医院信息管理系统（HIS）、电子病历（EMR）、医学影像信息系统（PACS）等多元系统已实现广泛部署，但传统网络架构存在的带宽不足、时延较高、多网隔离等问题，逐渐成为制约信息化深化应用的瓶颈。例如，医学影像数据的高清化、三维重建及 AI 辅助诊断需求，对网络传输速率提出了更高要求；远程手术、实时监护等新兴医疗场景，需要网络具备超低时延与超高可靠性；而医院内办公网、设备网、物联网等多网络并存的现状，导致信息孤岛现象突出，数据共享效率低下，难以支撑全流程精细化管理。在此背景下，传统通信技术已无法匹配现代医院信息化管理的多元化、高要求业务场景，亟需新一代通信技术提供支撑。^①

与此同时，人口老龄化加剧、医疗资源分布不均等社会问题日益凸显，进一步推动了医院信息化转型的进程。据相关数据显示，我国老年人口数量持续增长，慢性病患者群体不断扩大，对长期医疗照护、远程诊疗等服务的需求大幅提升。而优质医疗资源多集中于大城市核心医院，基层医疗机构服务能力相对薄弱，供需失衡问题显著。新一代通信技术的融入，能够打破空间限制，实现优质医疗资源的跨区域共享，推动分级诊疗体系落地，为解决医疗资源分配不均问题提供技术路径，这也成为医院信息化管理升级的重要驱动力。

① 白燕文：“互联网+”背景下公立医院财务信息化管理的现实需求及关键路径[J]. 中国管理信息化, 2025, 28(24): 215-217.

（二）新一代通信技术的迭代与产业赋能

通信技术历经多代演进，已从最初的语音服务阶段、互联网服务阶段，迈入无所不在的信息基础设施阶段。当前，5G 技术已进入大规模商用第五个年头，5G-A（5.5G）技术持续迭代，6G 标准化工作正式启动，F5G（第五代固定网络）等技术同步发展，形成了多技术协同演进的新一代通信技术体系。与传统通信技术相比，新一代通信技术在带宽、时延、连接数、感知能力等方面实现了质的飞跃，具备大带宽、低时延、高可靠、海量连接、通感融合等核心优势，能够精准匹配医院信息化管理中的高并发、高实时性、多终端接入等业务需求。

从产业政策导向来看，国家高度重视新型基础设施建设与数字健康发展。中共中央总书记习近平在主持中共中央政治局第三十四次集体学习时强调，要加快建设高速泛在、天地一体、云网融合、智能敏捷、绿色低碳、安全可控的智能化综合性数字信息基础设施，打通经济社会发展的信息“大动脉”。这一要求为新一代通信技术与医疗行业的融合发展指明了方向。同时，工业和信息化部等部门持续推进 5G、6G、F5G 等技术的研发与产业化落地，出台多项政策支持智慧医院建设，为新一代通信技术在医院信息化管理中的应用提供了良好的政策环境与产业基础。在技术成熟度与政策支持的双重驱动下，新一代通信技术与医院信息化管理的深度融合已成为必然趋势。

（三）医院信息化管理面临的现实挑战

尽管我国医院信息化建设已取得一定成效，但在实际管理过程中仍面临诸多挑战。其一，数据安全风险凸显。医院数据包含患者隐私信息、医疗记录、药品器械信息等敏感内容，传统网络架构的安全防护能力不足，易遭受黑客攻击、数据泄露等风险，严重威胁患者权益与医院声誉。其二，运维管理难度较大。医院网络覆盖范围广、终端类型多，包括医疗设备、办公终端、物联网设备等，传统运维模式依赖人工操作，效率低下，难以实现对网络状态的实时监测与故障的快速排查。其三，业务扩展性不足。随着医疗技术的发展，远程手术、AI 辅助诊疗、数字孪生医院等新兴业务不断涌现，传统通信网络架构僵化，难以快速适配新业务的部署需求，制约了医院信息化管理的创新发展。这些现实挑战进一步凸显了引入新一代通信技术的紧迫性与必要性。

二、研究意义

（一）理论意义

首先，丰富新一代通信技术在垂直行业应用的理论体系。当前，关于新一代通信技术研究多集中于技术研发与宏观产业应用层面，针对医疗行业尤其是医院信息化管理场景的系统性研究相对匮乏。本研究聚焦新一代通信技术与医院信息化管理的融合场景，深入分析技术应用的适配性与核心逻辑，能够填补相关领域的研究空白，为新一代通信技术在垂直行业的深度应用提供理论参考。其次，完善智慧医院信息化管理的理论框架。新一代通信技术的融入，推动医院信息化管理从传统的“业务数字化”向“管理智能化”转型，本研究通过梳理技术应用对医院管理流程、服务模式的重塑作用，能够丰富智慧医院建设的理论内涵，为医院信息化管理的升级方向提供理论指引。最后，为跨学科融合研究提供范例。新一代通信技术在医院信息化管理中的应用涉及通信工程、计算机科学、医学管理等多个学科领域，本研究通过多学科视角的融合分析，能够为跨学科研究提供方法论参考，推动相关学科的交叉创新。

（二）实践意义

其一，提升医院管理效能与服务质量。新一代通信技术的大带宽特性能够支撑医学影像、电子病历等海量数据的高速传输与实时共享，解决信息孤岛问题；超低时延与高可靠特性能够保障远程手术、实时监护等关键医疗场景的稳定运行，降低医疗风险；海量连接与无源物联技术能够实现对患者、医疗物资、环境等关键要素的全面感知与精准管理，提升管理的精细化水平。例如，5G-A 无源物联技术在医院的应用，可实现患者异常行为的秒级感知、医疗物资的全流程溯源，资产盘点效率提升约 50%，显著降低了管理成本与病患意外风险。其二，优化医疗资源配置效率。通过新一代通信技术构建的远程医疗网络，能够实现优质医疗资源的跨区域辐射，推动基层医疗机构与核心医院的协同诊疗，缓解医疗资源分布不均问题。同时，基于技术支撑的 AI 辅助诊断、智能分诊等系统，能够提升诊疗效率，缩短患者等待时间，改善就医体验。其三，推动医疗行业创新发展。新一代通信技术与 AI、大数据、数字孪生等技术的融合，能够催生远程手术机器人、数字孪生手术室、AI 辅助诊疗平台等新兴应用场景，推动医疗服务模式与管理模式的创新。例如，F5G 全光网支撑的一体化手术室建设，能够实现手术

直播、全息录播、远程协作等功能，为医疗教学与技术推广提供支撑；6G 的感知融合、天地一体化能力，有望实现偏远地区的医疗信号全覆盖，进一步拓展医疗服务的覆盖范围。其四，强化医疗数据安全防护。新一代通信技术具备的内生安全机制与加密能力，能够提升医院网络的安全防护水平，有效防范数据泄露、黑客攻击等风险，保障患者隐私与医院数据安全，维护医疗行业的公信力。

第二节 新一代通信技术的核心特征与演进趋势

一、核心特征

（一）多技术协同，构建全场景覆盖网络

新一代通信技术并非单一技术体系，而是由 5G/5G-A、F5G、6G、量子通信等多种技术协同构成的综合性网络体系，能够实现有线与无线、地面与空间的全场景覆盖。其中，5G/5G-A 技术以无线通信为核心，具备广覆盖、高移动性优势，适用于移动医疗、远程监护等场景；F5G 技术以全光网络为基础，具备大带宽、低时延、高安全特性，适用于医学影像传输、数据中心互联、一体化手术室等固定场景，与 5G 形成协同互补关系；6G 技术则致力于实现“空天地”一体化覆盖，通过卫星、无人机与地面网络的融合，解决偏远地区、特殊环境的通信覆盖问题；量子通信技术凭借绝对安全的加密特性，为医疗敏感数据的传输提供了安全保障。这种多技术协同的网络架构，能够精准匹配医院内不同场景的通信需求，实现全流程、无死角的网络覆盖。

（二）性能跃升，突破传统技术瓶颈

相较于传统通信技术，新一代通信技术在核心性能指标上实现了量级跃升，主要体现在以下方面：一是超大带宽。5G 的峰值速率可达 10Gbps，5G-A 提升至 100Gbps，6G 的太赫兹通信单链路峰值速率更是达到 500Gbps（为 5G 的 50 倍），能够轻松支撑 4K/8K 高清医学影像、三维重建数据等大流量数据的传输需求。F5G 技术以 10G PON、200G/400G OTN 等技术为核心，实现了千兆级的接入带宽与 T 比特级的传输能力，为医院数据中心的海量数据交互提供支撑。二是超低时延。5G 的端到端时延低至 1 毫秒，5G-A 进一步降至 0.1 毫秒，6G 时延可达到微秒级，能够满足远程手术、实时监护、设备协同控制等对时延要求极高的医

疗场景需求。例如，空芯光纤技术的应用，实现了跨地域数据中心间双向时延低至 0.93 毫秒的业界最低水平，为远程医疗的精准协同提供了保障。三是海量连接。5G 支持每平方公里百万级的连接数，5G-A 与 6G 的连接能力进一步增强，能够支撑医院内呼吸机、心电监护仪、可穿戴设备、环境传感器等海量物联网设备的同时接入，实现“万物互联”的管理目标。四是超高可靠。新一代通信技术通过多链路冗余、智能容错等机制，实现了 99.999% 以上的可靠性，能够保障关键医疗设备与系统的连续稳定运行，降低因网络中断导致的医疗风险。

（三）多能力融合，拓展服务边界

新一代通信技术突破了传统通信仅提供连接服务的局限，实现了通信、感知、计算、AI、安全等多能力的深度融合，拓展了技术的服务边界。一是通感融合。通过基站信号的回波感知环境信息，使网络不仅具备通信能力，还具备感知能力。例如，6G 的通感融合技术能够实现对医院内人员位置、移动轨迹、环境状态的精准感知，为患者管理、安防监控提供支撑；紫金山实验室构建的通感融合外场试验网，已实现对低空目标的精准感知，有望应用于医疗应急救援场景。二是算网融合。将边缘算力部署于基站或网络节点，实现算力资源的就近调度，为 AI 辅助诊断、实时数据处理等应用提供算力支撑。例如，AI-Native Network（智能原生网络）通过分布式组网与算网融合机制，能够为医院的 AI 辅助阅片、智能分诊等系统提供低时延的算力服务，提升诊疗效率。三是通质融合。将 AI 技术嵌入网络内部，实现网络的智能自治与优化，能够根据医疗业务的需求动态调整网络资源，提升网络的适配性与运行效率。四是天地融合。通过卫星、无人机与地面网络的协同，实现全域无缝覆盖，解决偏远地区、应急场景的医疗通信问题。例如，6G 的 NTN（非地面网络）技术能够实现手机与卫星的直接连接，在地面网络中断的情况下保障医疗通信的连续性，为应急救援提供支撑。

（四）绿色智能，适配行业发展需求

新一代通信技术在发展过程中注重绿色低碳与智能运维，适配医院等公共服务机构的发展需求。在绿色低碳方面，通过技术创新降低设备功耗，例如，1.6T 光模块采用量子点激光器技术实现功耗降低 40%，F5G 全光网架构相较于传统以太网网架构能耗显著降低，符合医院的绿色发展理念。在智能运维方面，新一代通信技术具备网络可视化、自动化管理能力，能够实现对网络状态的实时监测、故障的智能诊断与自动修复。例如，F5G 全光网的网管系统能够提供基础业务监控、

告警管理、自动化报表等功能，将运维人员从复杂的工作中解放出来，提升运维效率；AI 与网络的深度融合实现了网络的智能自治，能够自主感知用户与环境需求，最优配送资源，降低运维成本。此外，无源物联技术的应用，使物联网标签无需电池，通过吸收环境能量工作，具备低成本、免维护、易部署的优势，大幅降低了医院物联网设备的运维难度与成本。

（五）高安全性，保障敏感数据传输

医疗数据的敏感性决定了医院信息化管理对网络安全的高要求，新一代通信技术通过多种技术手段强化了安全防护能力。一是内生安全机制。在网络架构设计阶段融入安全理念，通过分布式组网、加密传输、身份认证等技术，构建全方位的安全防护体系。二是量子通信技术的应用。量子通信利用量子力学基本原理实现信息传输与加密，具备理论上的绝对安全性，能够有效防范窃听、破解等安全风险。例如，我国构建的量子安全基础设施与“点亮百城”量子试验网，为医疗敏感数据的传输提供了最高等级的安全保障。三是安全服务一体化。新一代通信技术将安全服务纳入整体信息服务体系，通过网络提供实时的安全监测、风险预警、应急响应等服务，提升医院网络的安全防护水平，保障患者隐私与医院数据安全。

二、演进趋势

（一）技术能力持续升级，向“极致性能”演进

新一代通信技术的性能指标将持续向极致化方向演进，以满足日益增长的医疗业务需求。从速率来看，将从 5G 的 10Gbps、5G-A 的 100Gbps，逐步迈向 6G 的太赫兹通信 500Gbps，甚至更高速率，能够支撑全息医疗、元宇宙诊疗等更复杂的应用场景；从时延来看，将从 5G 的毫秒级降至 6G 的微秒级，为远程手术机器人的精准控制、神经信号的实时传输等极端场景提供支撑；从连接数来看，将实现从百万级/平方公里向亿级/平方公里的跨越，支撑更广泛的万物互联场景，实现医院内“人-机-物-环境”的全面互联；从定位精度来看，将从米级提升至厘米级、毫米级，能够实现对医疗设备、患者的精准定位与轨迹追踪，提升管理的精细化水平。同时，通感融合、算网融合等能力将进一步增强，实现通信与感知、计算的深度协同，为医疗场景提供更全面的技术支撑。

（二）网络架构迭代优化，向“智能原生”演进

新一代通信网络将从传统的“连接导向”向“智能原生”演进，网络与 AI 的融合将进入深度协同阶段。未来的网络架构将具备高度的柔性扩展与智能自治能力，能够根据医疗业务的动态需求自动调整网络资源配置，实现“业务驱动网络”的精准适配。例如，AI-Native Network 将 AI 能力嵌入网络的各个层级，实现网络的智能规划、智能运维、智能优化与智能安全，能够自主识别医疗业务类型（如远程手术、影像传输、日常办公），并匹配最优的网络策略；算力互联网的发展将实现全国范围内算力资源的“一盘棋”调度，医院能够根据需求便捷获取云端算力支撑，降低本地算力建设成本。同时，网络架构将向扁平化、云化方向发展，打破传统蜂窝架构的限制，通过无蜂窝智能化组网等创新技术，解决复杂环境下的网络干扰问题，提升网络的覆盖质量与运行效率。

（三）融合范围不断拓展，向“DOICT 超融合”演进

新一代通信技术的演进将推动 ICT（信息与通信技术）向 DOICT（数据技术、运营技术、信息技术和通信技术）超融合方向发展，实现多技术、多领域的深度融合。在技术融合层面，通信技术将与 AI、大数据、数字孪生、量子计算等技术深度协同，形成更强大的技术合力。例如，6G 与数字孪生技术的融合，能够构建医院的数字孪生模型，实现对医院运营状态的实时仿真、预测与优化；通信技术与具身智能的融合，能够支撑医疗机器人的远程控制与自主作业，提升医疗服务的自动化水平。在产业融合层面，通信技术将与医疗、制造、交通等多个行业深度融合，推动跨行业的协同创新。对于医疗行业而言，这种超融合趋势将实现医疗业务与网络技术、数据技术、运营技术的全面协同，例如，通过 DOICT 超融合架构支撑的医疗物资供应链管理，能够实现从采购、入库、使用到废弃的全流程智能化管理，提升供应链的运行效率与可靠性。同时，超融合架构将时间敏感特性和确定性特性嵌入整个系统，能够更好地适配医疗行业对实时性、确定性的严格要求。

（四）覆盖范围持续拓展，向“全域无缝”演进

新一代通信技术将突破传统地面网络的覆盖局限，向“空天地”一体化的全域无缝覆盖演进。5G 时代已开始研究非地面网络（NTN），6G 时代将实现“空天地”一体化体系架构的全面落地，通过卫星、无人机、地面基站的协同组网，实现全球范围内的通信覆盖。这种全域覆盖能力将为医疗行业带来革命性变化，能够解

决偏远地区、山区、海洋等传统网络无法覆盖区域的医疗通信问题，实现医疗服务的全域可达。例如，6G 的手机直连卫星技术，能够在地面网络中断的情况下，保障偏远地区患者的急救通信需求，实现远程会诊与指导；“空天地”一体化网络还能够支撑应急医疗救援场景的通信保障，提升灾害、事故等突发情况下的医疗救援效率。同时，覆盖范围的拓展将实现从“按人覆盖”向“按需覆盖”的转变，不仅满足人的通信需求，还能覆盖医院内的医疗设备、物资、环境等各类要素，支撑更广泛的万物互联场景。

（五）产业生态协同发展，向“标准化、规模化”演进

随着新一代通信技术的发展，相关产业生态将逐步完善，呈现标准化、规模化的演进趋势。在标准化方面，全球各国正积极推动 6G 等新一代通信技术的标准制定工作，我国 6G 专利申请量占全球 40.3% 居首，主导 14 项关键国际标准，为技术的规模化应用奠定了基础。同时，行业内正推动通信技术与医疗行业应用的标准化对接，制定适配医疗场景的技术规范与应用标准，提升技术应用的兼容性与通用性。在规模化方面，随着技术成熟度的提升与成本的降低，新一代通信技术在医院信息化管理中的应用将从试点示范走向规模化落地。例如，5G-A 无源物联、F5G 全光网等技术已在部分医院实现试点应用，未来将逐步推广至全国各级医疗机构；1.6T 光模块等核心组件的规模化部署，将进一步降低网络建设成本，推动技术的普及应用。此外，产业协同将进一步深化，通信企业、医疗设备企业、医院管理机构等各方将加强联动，形成从技术研发、产品制造到应用落地的全链条产业生态，推动新一代通信技术在医疗行业的深度融合与创新发展。

第三节 现代医院信息化管理的现存格局与核心挑战

一、现存格局

（一）分级分层建设不均衡，头部与基层差距显著

当前我国医院信息化建设呈现明显的“阶梯式”格局，三级医院与基层医疗机构（社区卫生服务中心、乡镇卫生院等）在建设水平、技术应用深度上存在巨大差距。头部三级医院凭借资金、技术与人才优势，已完成医院信息管理系统（HIS）、电子病历（EMR）、医学影像信息系统（PACS）等核心系统的全流程部署，部分领先医院已迈入电子病历 7 级以上水平，并开始探索 AI 辅助诊疗、

数字孪生手术室等智能化应用。例如，国内多家大三甲医院通过集成化信息平台实现了诊疗数据的初步整合，为临床决策提供数据支撑。与之形成鲜明对比的是，基层医疗机构信息化建设普遍滞后，约 40% 的乡镇卫生院仅完成基础挂号、收费系统部署，电子病历覆盖率不足 30%，缺乏与上级医院的数据互通能力，难以支撑分级诊疗体系的高效运转。这种不均衡格局导致优质医疗资源的数字化优势无法有效下沉，制约了全国医疗服务整体效能的提升。

（二）系统建设从“评级导向”向“服务导向”转型过渡期特征明显

过去较长一段时期，医院信息化建设多以满足评级硬指标为核心目标，形成了“功能堆砌”的建设模式。2025 年《全国医院信息化建设现状调研》显示，83% 的三级医院为适配电子病历分级评价、智慧服务评级等要求，在核心系统中新增了数据上报、流程留痕等冗余模块，其中仅 37% 的模块为医护实际诊疗所需。这种建设模式导致系统操作繁琐，医护人员开具处方、录入病历的时间显著增加，反而降低了诊疗效率。2025 年 6 月国家卫健委《医院信息化建设提质增效工作方案》发布后，行业开启“提质行动”，医院信息化建设逐步向“服务导向”转型。部分医院开始推进系统“瘦身”，通过流程优化、功能集成提升易用性，例如将诊断、处方、医嘱流程集成至同一界面，实现操作步骤从 5 步减至 1 步；患者端 APP 则简化为预约、缴费、查报告 3 个核心入口，老年患者使用率提升 27%。当前行业正处于转型过渡期，“评级遗留系统”与“服务型优化模块”并存，系统整合与流程重构任务艰巨。

（三）多系统并存但协同不足，数据孤岛现象尚未根本破解

现代医院信息化体系已形成多系统并行的复杂格局，除核心的 HIS、EMR、PACS 系统外，还涵盖实验室信息系统（LIS）、医院资源规划系统（HRP）、供应链管理系统、安防监控系统等数十个专项系统。但由于不同系统建设周期不同、技术标准不统一，多数医院存在“多网隔离、数据割裂”的问题。例如，临床诊疗数据分散存储于 EMR、PACS 等不同系统，无法实现一键调取与综合分析；物资管理数据与临床使用数据脱节，导致库存积压与短缺问题并存。尽管近年来国家推动医疗健康信息互联互通标准化成熟度测评，但仍有超过 50% 的医院未实现核心系统的数据互通，数据孤岛成为制约医院精细化管理与智能化升级的核心障碍。同时，患者端多平台并存现象突出，部分医院同时运行 APP、微信公众号、支付宝生活号等多个服务入口，功能重复且数据不通，增加了患者使用成本与医院运维负担。

（四）智能化应用处于“单点试点”向“规模化落地”过渡阶段

随着 AI、大数据技术的发展，医院信息化智能化应用探索不断深入，但整体仍处于“单点突破、零星试点”状态。目前应用主要集中于影像阅片、智能分诊、病历结构化录入等标准化程度较高的场景，例如 AI 辅助肺结节检测、糖尿病视网膜病变筛查等已在部分医院试点应用，准确率可达 95% 以上。但这些应用多为独立模块，未与临床诊疗流程深度融合，难以充分发挥价值。在医院管理领域，智能化应用更为滞后，除少数领先医院尝试用 AI 进行运营数据分析外，多数医院仍依赖人工进行资源调度、成本核算、风险管控。此外，“小而美”的轻量化应用成为新趋势，如医嘱模板小程序、患儿信息可视化卡片等工具因适配性强、部署成本低受到医护人员青睐，但这类应用缺乏统一规划，易形成新的“应用孤岛”，难以支撑医院管理的系统性升级。

二、核心挑战

（一）系统易用性不足与医护适配性矛盾突出

这是当前医院信息化管理最直观的挑战。评级导向下的系统设计忽视了医护人员的实际操作需求，导致界面复杂、流程繁琐。例如，部分电子病历系统要求医护人员录入大量非诊疗核心的评级字段，漏填即会导致单据退回；多系统切换频繁，医护人员需在 EMR、PACS、LIS 等系统间反复登录查询，分散了诊疗注意力。2025 年行业调研显示，三级医院医护人员日均系统操作时长超过 2 小时，其中 40% 的操作与直接诊疗无关。这种“技术反噬效率”的现象导致医护人员对信息化系统的抵触情绪，部分医院甚至出现专人“代填评级数据”的极端情况，违背了信息化建设的初衷。同时，系统更新迭代与医护培训不同步，约 30% 的医护人员对新增功能掌握不足，进一步降低了系统使用效能。^①

（二）数据治理能力薄弱，难以支撑价值化应用

医院数据涵盖临床诊疗、运营管理、患者行为等多个维度，体量巨大但质量参差不齐，数据治理成为制约信息化深化应用的关键瓶颈。一是数据标准化程度低，不同系统、不同科室的数据编码不统一，如药品名称、疾病诊断存在多种表述方式，导致数据整合困难；二是数据完整性不足，诊疗过程中的非结构化数据

① 何菁华. 信息化时代医院工会管理创新与改革实践探索 [J]. 中国信息界, 2025, (11): 198-200.

（如医生口述记录、手写批注）难以转化为结构化数据，数据缺失率较高；三是数据质量管控缺失，缺乏统一的数据校验与清洗机制，部分数据存在错误、重复等问题。薄弱的数据治理能力导致医院难以开展深度数据分析，无法将海量数据转化为支撑临床决策、优化管理流程的有效价值，智能化应用也因数据基础薄弱而难以落地。

（三）运维管理体系滞后，难以适配复杂信息系统需求

随着医院信息化系统的日益复杂，运维管理难度大幅提升，传统运维模式已无法满足需求。一是运维团队配置不足，多数医院信息科人员占比不足全院职工的1%，面对数十个系统、数千台终端的运维需求，难以实现全时段、全覆盖的保障；二是运维技术手段落后，仍以人工排查、被动响应为主，无法实现对系统性能、网络状态的实时监测，故障发现与修复周期长，部分系统故障会导致诊疗流程中断；三是运维成本高企，多系统并行导致运维接口繁杂，第三方运维服务费用逐年攀升，基层医院难以承担。此外，物联网设备的普及进一步增加了运维压力，医院内呼吸机、监护仪、物联网标签等终端数量激增，设备故障排查与网络调试工作量呈指数级增长。

（四）安全防护体系不健全，数据隐私风险凸显

医疗数据包含患者隐私信息、诊疗记录等敏感内容，其安全防护直接关系到患者权益与医院声誉。当前医院信息化安全防护存在多重漏洞：一是安全防护技术滞后，部分医院仍依赖传统防火墙、杀毒软件等基础防护手段，缺乏对数据传输、存储、使用全流程的加密保护，易遭受黑客攻击与数据泄露；二是安全管理机制不完善，缺乏统一的安全管理制度与应急响应预案，员工安全意识薄弱，存在违规操作、密码泄露等人为风险；三是多系统接入增加安全隐患，物联网设备、第三方服务平台的接入扩大了攻击面，部分低成本物联网设备缺乏安全设计，成为网络安全的薄弱环节。近年来，医疗数据泄露事件频发，2025年上半年全国共通报医疗行业数据安全事件32起，涉及患者信息超10万条，凸显了安全防护的紧迫性。

（五）建设资金与人才短缺，基层医院发展动力不足

资金与人才短缺是制约基层医院信息化发展的核心瓶颈。在资金方面，医院信息化建设前期投入大、回报周期长，基层医院运营资金紧张，难以承担系统采购、升级与运维费用。某省二甲医院为冲刺电子病历5级，投入200万元采购新

系统后，因后续运维资金不足导致系统无法充分发挥作用。在人才方面，医疗信息化人才需具备医疗业务、信息技术、管理科学等跨学科知识，这类人才多向大城市三甲医院集聚，基层医院信息科人员多为兼职或转岗，缺乏专业培训，难以支撑信息化系统的深度应用与优化升级。资金与人才的双重短缺，导致基层医院信息化建设陷入“投入不足—应用效果差—不愿再投入”的恶性循环，进一步加剧了行业发展不均衡。

第四节 通信技术与医院管理深度融合的创新价值与应用逻辑

一、创新价值

（一）重构诊疗服务流程，提升医疗服务效率与体验

通信技术与医院管理的深度融合，能够打破传统诊疗流程的时空限制与环节壁垒，实现服务流程的革命性重构。在临床诊疗环节，5G、F5G 等技术的大带宽、低时延特性支撑高清医学影像、远程会诊数据的实时传输，使远程手术、多学科联合诊疗（MDT）突破地域限制；AI 辅助诊疗系统通过高速网络对接云端算力，实现诊疗数据的实时分析与诊断建议推送，缩短诊断周期。在患者服务环节，基于无源物联、移动通信技术的智慧服务体系，能够实现从预约挂号、候诊提醒、报告查询到出院随访的全流程线上化与智能化。例如，医院通过短信或 APP 推送实时候诊信息，患者可精准安排就诊时间，避免诊室门口扎堆等待；出院后通过远程监测设备与网络连接，医护人员可实时掌握患者康复情况，及时调整康复方案。这些创新应用不仅将医护人员从繁琐的事务性工作中解放出来，提升诊疗效率，更能显著降低患者就医等待时间，改善就医体验。

（二）破解数据孤岛难题，赋能精细化管理与智能决策

新一代通信技术构建的高速、稳定、全覆盖网络，是打破数据孤岛、实现数据价值化的核心支撑。通过 F5G 全光网与 5G 协同组网，能够实现医院内 HIS、EMR、PACS、HRP 等多系统的高速互联，建立统一的数据交换平台，实现诊疗数据、运营数据、物资数据的全维度整合。在此基础上，通过算网融合技术将云端算力与本地数据结合，能够开展多维度数据分析，为医院管理提供精准决策支撑。例如，在运营管理方面，通过分析诊疗数据与资源占用数据，优化科室排班

与设备调度，降低运营成本；在物资管理方面，通过物联网设备与高速网络的联动，实现医疗耗材的全流程溯源与库存动态监控，避免积压与短缺；在质量管控方面，通过诊疗数据的实时采集与分析，及时发现诊疗风险点，提升医疗质量安全水平。某医院通过通信技术实现数据整合后，运营成本降低 15%，医疗差错率下降 20%，充分体现了数据驱动管理的创新价值。

（三）优化医疗资源配置，推动分级诊疗体系落地

通信技术能够打破医疗资源的地域限制，构建“核心医院—基层医疗机构”的数字化协同体系，为分级诊疗落地提供技术保障。通过 5G 远程医疗网络，核心医院的优质医疗资源可实现跨区域辐射，基层医疗机构能够实时获取上级医院的诊疗指导、远程会诊等服务，提升基层诊疗能力。例如，偏远地区乡镇卫生院通过高清视频会诊系统与县级医院对接，实现常见病、慢性病的精准诊断，避免患者盲目转诊；核心医院通过远程手术指导系统，协助基层医院开展复杂手术，提升基层医疗服务水平。同时，通信技术支撑的区域医疗数据平台，能够实现患者健康档案在不同层级医疗机构间的互联互通，使患者在基层就诊时可直接调取上级医院的诊疗记录，避免重复检查，降低医疗费用。这种资源配置模式的创新，能够有效缓解优质医疗资源集中于大城市核心医院的现状，推动医疗资源下沉，提升全国医疗服务整体均衡性。

（四）升级运维与安全体系，保障医院管理稳定高效运行

通信技术的融入能够推动医院运维与安全管理模式的智能化升级，提升管理的稳定性与可靠性。在运维管理方面，基于 5G-A 通感融合技术与物联网设备，能够实现对医院网络、服务器、医疗设备等核心资产的实时监测与状态感知，通过 AI 算法实现故障的提前预警与智能诊断，将传统“被动维修”转变为“主动运维”。例如，F5G 全光网的网管系统可提供全流程可视化监控，实现告警管理与自动化报表生成，将运维人员从繁琐的人工操作中解放出来，运维效率提升 50% 以上。在安全管理方面，区块链技术、5G 内生安全等技术能够构建全流程安全防护体系，实现数据传输、存储、使用的全链路加密保护；通过安全态势感知系统与高速网络的联动，能够实时监测网络攻击与数据泄露风险，及时启动应急响应机制。这些创新应用为医院信息化系统的稳定运行与数据安全提供了全方位保障，维护医疗行业公信力。

（五）催生新兴医疗业态，推动医疗行业高质量发展

通信技术与医院管理的深度融合，能够催生远程手术机器人、数字孪生医院、全息医疗等一系列新兴医疗业态，推动医疗行业向智能化、精准化方向转型。数字孪生技术通过高速网络整合医院建筑、设备、诊疗流程等多维度数据，构建虚拟仿真模型，可用于医院规划设计、流程优化与应急演练，降低建设与运营风险；全息医疗借助 5G-A 大带宽技术实现医学影像的全息呈现，为远程会诊与医疗教学提供更直观的支撑；具身智能机器人通过网络与云端控制系统联动，能够实现病房巡检、药品配送、患者护理等自动化服务，缓解医护人员短缺压力。这些新兴业态不仅拓展了医疗服务的边界，更推动了医疗技术、管理模式的创新突破，为医疗行业高质量发展注入新动能。

二、应用逻辑

（一）需求导向：以临床与管理痛点为核心适配技术方案

通信技术与医院管理融合的核心应用逻辑是“需求驱动技术选型”，避免技术与业务脱节。医院需基于自身诊疗特色、管理痛点与发展阶段，精准匹配通信技术方案。对于大三甲医院，应聚焦复杂手术远程指导、AI 辅助精准诊疗、多系统数据整合等高端需求，采用 5G-A、F5G 全光网、算网融合等技术，构建高性能、高可靠的一体化信息平台；对于基层医疗机构，应优先解决基础数据互通、远程会诊接入、简单智慧服务等核心需求，采用低成本、易部署的 5G 物联网、轻量化数据终端等技术方案，实现与上级医院的高效协同。例如，针对基层医院影像诊断能力不足的痛点，通过 5G 网络对接上级医院 PACS 系统，实现影像数据的实时上传与远程诊断，无需投入巨资建设本地影像诊断中心；针对大三甲医院手术教学需求，通过 F5G 全光网支撑手术场景的 4K/8K 高清直播，实现多地点同步教学。^①

（二）分步实施：从基础网络构建到智能化深度应用梯度推进

通信技术与医院管理的融合是系统工程，需遵循“分步实施、梯度推进”的逻辑，避免盲目求全求快。第一阶段以基础网络升级为核心，构建覆盖全院的高速、稳定通信网络。重点推进 F5G 全光网建设，实现门诊、住院部、手术室等核心区域的有线网络全覆盖；部署 5G 基站，支撑移动医疗设备、物联网终端的

① 鲁慧. 医院档案信息化管理创新模式 [J]. 数字技术与应用, 2025, 43 (11): 100-102.

无线接入，打通数据传输的“大动脉”。第二阶段开展系统整合与数据治理，基于基础网络构建统一的数据交换平台，完成现有 HIS、EMR、PACS 等系统的接口改造与数据标准化处理，打破数据孤岛。第三阶段推进智能化应用落地，在基础网络与数据整合的基础上，部署 AI 辅助诊疗、智能运维、智慧服务等应用模块，实现从“数字化”向“智能化”的升级。例如，某医院通过“网络升级—数据整合—智能应用”三步法，用 3 年时间完成信息化升级，避免了一次性大规模投入带来的资金压力与技术风险，确保每个阶段的建设成果都能有效服务于临床与管理。

（三）协同联动：构建“医院—技术提供商—监管部门”多方协同生态

通信技术与医院管理的深度融合，需要医院、通信技术提供商、医疗设备企业、监管部门等多方主体协同联动，构建良性产业生态。医院作为应用主体，需明确自身需求，主导应用场景设计与落地验证，同时加强医护人员培训，提升技术接受度与应用能力；通信技术提供商应深入了解医疗行业特性，开发适配医疗场景的定制化技术方案，加强技术迭代与售后服务，保障系统稳定运行；医疗设备企业需推动设备的网络化、智能化升级，实现与医院信息系统的无缝对接；监管部门则应完善相关标准与政策，规范数据安全与隐私保护，为融合发展提供制度保障。例如，在远程手术机器人应用场景中，医院提出临床需求，通信企业提供低时延网络保障，设备企业研发适配网络的机器人系统，监管部门制定手术安全与数据安全标准，多方协同确保应用的安全性、有效性。这种协同生态能够整合各方资源，破解技术应用中的各类壁垒，推动融合应用的规模化落地。

（四）安全可控：建立全流程安全保障体系贯穿融合全过程

医疗数据的敏感性决定了“安全可控”是通信技术与医院管理融合的前提条件，需将安全保障体系贯穿于技术选型、系统建设、应用运营的全流程。在技术选型阶段，优先采用具备内生安全机制的通信技术，如量子通信、5G 安全切片等，从源头提升安全防护能力；在系统建设阶段，构建“网络安全—数据安全—终端安全”的全方位防护体系，部署防火墙、入侵检测系统、数据加密设备等安全组件，实现对数据传输、存储、使用全链路的保护；在应用运营阶段，建立常态化安全监测与应急响应机制，通过 AI 安全态势感知系统实时监测网络攻击与数据泄露风险，定期开展安全演练，提升应急处置能力。同时，加强人员安全管理，定期开展安全培训，规范操作流程，避免人为安全风险。例如，某医院在部署 5G 远程医疗系统时，采用网络切片技术将医疗数据传输与普通办公网络隔离，同时通过量子加密技术保障数据传输安全，确保患者隐私与诊疗数据安全可控。

第二章 5G 技术在医院信息化管理中的深度应用研究

第一节 5G 技术特点及其医疗场景适配性分析

一、5G 技术核心特点解析

（一）增强移动宽带（eMBB）：超高带宽支撑海量数据传输

5G 技术的增强移动宽带特性是其区别于前代通信技术的核心优势之一，其峰值速率可达 10Gbps 以上，是 4G 网络的 100 倍，单用户平均速率也能稳定在 1Gbps 左右。这一特性实现了从“万物互联”到“万物智联”的数据传输基础支撑，能够轻松应对高清视频、大容量文件的实时传输需求。与 4G 网络相比，5G 的频谱效率大幅提升，通过采用 Massive MIMO（大规模天线）、超密集组网等关键技术，在单位面积内能够提供更高的网络容量，有效解决了高密度场景下的网络拥堵问题。在数据传输模式上，5G 支持全双工通信，实现了上行与下行数据的同步传输，打破了传统通信技术的传输时序限制，为实时交互类应用提供了技术保障。

（二）超高可靠低时延通信（URLLC）：毫秒级响应保障关键操作

超高可靠低时延通信是 5G 技术针对垂直行业关键应用场景设计的核心特性，其端到端时延可低至 1-10ms，可靠性高达 99.999%。这一特性彻底突破了传统通信技术的时延瓶颈，实现了接近“实时”的信号传输与反馈。在技术实现上，5G 通过缩短传输时隙、优化网络架构、采用边缘计算等方式，最大限度降低了信号传输过程中的延迟与丢包率。相较于 4G 网络 50-100ms 的时延，5G 的低时延特性使得远程控制、实时监测等对时间敏感的应用成为可能，尤其在涉及生命安全的医疗场景中，这一特性直接决定了技术应用的可行性与安全性。

（三）海量机器类通信（mMTC）：高密度连接支撑全场景互联

海量机器类通信特性赋予了 5G 网络超强的终端接入能力，其单小区连接密

度可达 100 万 / 平方公里，是 4G 网络的 10 倍。这一特性能够满足物联网时代海量智能终端的同时接入需求，实现“人 - 机 - 物”的全要素互联。5G 网络通过采用窄带传输、轻量化协议等技术，在保障连接数量的同时，有效降低了终端设备的功耗与成本，尤其适配无源物联网设备的应用需求。在复杂场景下，5G 网络能够实现对不同类型终端的差异化资源管理，为高优先级设备分配更多网络资源，确保关键数据的优先传输，为全场景智能化管理提供了网络支撑。

（四）网络切片技术：定制化网络保障场景差异化需求

网络切片是 5G 技术的革命性创新，通过将物理网络在逻辑上划分为多个相互隔离的虚拟网络，实现了“一网多用”的灵活部署。每个网络切片可根据具体应用场景的需求，定制化配置带宽、时延、可靠性等网络参数，不同切片之间互不干扰，确保了关键应用场景的网络资源独占性。在技术架构上，网络切片涵盖接入网切片、核心网切片与传输网切片，能够实现全链路的资源定制与隔离。这一特性使得 5G 网络能够同时适配不同类型的医疗应用场景，既可为远程手术等关键场景提供高可靠低时延的专属网络，也可在日常办公、患者服务等场景提供高效经济的网络资源，大幅提升了网络的适配性与资源利用效率。

二、5G 技术与医疗场景的适配性分析

（一）与海量医疗数据传输场景的适配性

医疗行业是典型的“数据密集型”行业，医学影像、电子病历、基因测序等数据具有体量大、精度高、实时性要求高等特点，与 5G 增强移动宽带特性形成精准适配。以医学影像数据为例，单幅 CT 图像数据量可达数 MB，一次全身 MRI 检查生成的影像数据甚至超过 1GB，传统 4G 网络在传输这类数据时，常出现卡顿、延迟或压缩失真等问题，影响诊断准确性。5G 技术的 10Gbps 超宽带宽能够实现 4K/8K 超高清医学影像的无损实时传输，甚至支持 360 度术野画面的同步回传，让医生能够获取更清晰、完整的临床信息。在基因测序场景中，单次基因测序会产生数十 GB 的原始数据，5G 网络能够快速完成数据上传与云端分析，将基因诊断周期从数天缩短至数小时，为精准医疗提供高效数据支撑。此外，多学科联合诊疗（MDT）场景中，来自不同科室的诊疗数据、影像资料需要实时共享，5G 网络的高带宽与全双工通信特性能够保障多终端、多数据类型的同步交互，

提升诊疗协同效率。^①

（二）与关键医疗操作场景的适配性

远程手术、实时监护、院前急救等关键医疗场景对网络的时延与可靠性要求极高，5G 超高可靠低时延通信特性能够精准匹配这类场景的需求。在远程手术场景中，手术机器人的操作指令与反馈信号需要实时传输，时延超过 20ms 就可能导致操作误差，威胁患者生命安全。5G 技术 1-10ms 的毫秒级时延能够实现操作指令与机械臂动作的同步响应，某三甲医院的测试数据显示，通过 5G 网络进行跨城市远程手术，指令传输时延稳定在 8ms 以内，手术效果与现场操作无显著差异。在实时监护场景中，重症患者的生命体征数据需要持续、准确地传输至监护中心，5G 的高可靠性能够确保数据传输的连续性与完整性，丢包率低于 0.001%，有效避免了因数据丢失导致的病情误判。在院前急救场景中，急救车上的生命体征监测设备、现场视频采集设备需要将数据实时回传至医院急诊科，5G 的低时延特性能够让医院提前启动抢救预案，将患者从入院到开始抢救的时间缩短 30% 以上，为危重患者争取“黄金抢救时间”。

（三）与全场景智能化管理场景的适配性

随着智慧医院建设的推进，医院内的智能设备数量呈指数级增长，涵盖患者监护、药品管理、物流配送、环境监测等多个环节，5G 海量机器类通信特性能够为这类全场景智能化管理场景提供支撑。单家大型医院的联网智能设备数量已突破万台，传统 4G 网络的连接密度难以满足需求，常出现设备“抢带宽”导致的通信中断。5G 网络 100 万 / 平方公里的高密度连接能力，能够实现所有智能设备的同时稳定接入，某智慧医院通过 5G 网络接入 5000 余台智能设备，设备在线率从 4G 时代的 85% 提升至 99.9%。在药品管理场景中，搭载 5G 物联网模块的药品标签能够实时上传药品位置、有效期、库存数量等信息，实现药品全流程溯源；在物流配送场景中，5G 导航机器人能够实时接收调度指令，精准完成药品、耗材的院内配送，提升物流效率。此外，5G 的低功耗特性能够延长物联网设备的续航时间，降低设备维护成本，尤其适配长期部署的监测类设备。

（四）与多场景差异化需求场景的适配性

医院内不同应用场景对网络的需求差异显著，远程手术需要高可靠低时延，

^① 任旭,陈勇,杨秀兰,等.5G 背景下急诊急救体系建设的现状与展望[J].中国急救医学,2025,45(08): 723-726.

日常办公需要高效经济的带宽，患者上网需要稳定的接入体验，5G 网络切片技术能够精准适配这类差异化需求。通过构建多个相互隔离的网络切片，医院可为不同场景定制专属网络资源：为远程手术、实时监护等关键场景分配高优先级切片，保障 1ms 低时延与 99.999% 可靠性；为医学影像传输、远程会诊等场景分配大带宽切片，满足高清数据传输需求；为日常办公、患者上网等场景分配通用切片，优化网络资源利用效率。网络切片技术还能够实现网络资源的动态调整，根据场景需求的变化实时分配带宽与时延资源，例如在手术高峰期手术室切片扩容，在就诊低谷期为办公切片释放资源。这种定制化的网络服务模式，既保障了关键场景的网络质量，又提升了整体网络资源的利用效率，为医院信息化管理的多元化需求提供了灵活支撑。

第二节 5G 在远程精准诊疗中的创新应用

一、5G+ 远程手术：突破空间限制的精准操作

（一）远程手术机器人协同操作应用

5G 技术与手术机器人的深度融合，构建了跨地域的远程手术协同体系，实现了优质医疗资源的跨区域辐射。在技术架构上，远程手术系统由主操作端、5G 传输网络、从操作端（手术机器人）三部分组成，主刀医生通过主操作端发出操作指令，指令经 5G 网络实时传输至从操作端，手术机器人根据指令完成精准操作，同时将手术部位的影像与力反馈信号同步回传至主操作端。5G 网络的低时延特性确保了操作指令与机器人动作的同步响应，力反馈信号的实时传输让医生能够精准感知手术部位的组织硬度、阻力等信息，保障手术操作的精准性。某医疗团队利用 5G 技术完成了跨城市的骨科机器人辅助手术，主刀医生在省会医院操作，机械臂在 200 公里外的县级医院执行骨折复位，手术时间较传统方式缩短 30%，患者创伤更小，术后恢复周期缩短 50%。目前，5G 远程手术已在骨科、泌尿外科、普外科等多个领域开展应用，尤其为偏远地区缺乏优质医疗资源的患者提供了高端手术服务，推动了医疗资源的均衡配置。

（二）多中心联合远程手术指导应用

针对复杂疑难手术场景，5G 技术构建了多中心联合远程手术指导体系，实现了多位专家对单一手术的协同指导。在手术过程中，主刀医生所在的手术室通

过 5G 网络将 4K 超高清手术影像实时传输至多个专家终端，专家可通过终端实时观察手术进展，通过语音、文字或 AR 标注等方式提出指导建议，指导信息经 5G 网络实时反馈至手术室，辅助主刀医生完成复杂操作。5G 网络的高带宽特性保障了超高清手术影像的流畅传输，AR 标注功能让专家能够精准定位病灶位置、标注手术关键路径，提升指导的直观性与有效性。某三甲医院在开展一台复杂的颅内肿瘤切除手术时，通过 5G 网络联动北京、上海两家医院的神经外科专家进行远程指导，专家通过 AR 眼镜标注肿瘤边界与重要神经位置，主刀医生根据标注完成精准切除，手术成功率大幅提升。这种多中心联合指导模式，整合了全国优质医疗资源，为疑难手术提供了多学科协同支撑，降低了手术风险，提升了基层医院的复杂手术开展能力。

二、5G+ 远程影像诊断：全流程精准化分析

（一）超高清医学影像远程实时解读

5G 技术突破了传统远程影像诊断的带宽限制，实现了超高清医学影像的远程实时解读，提升了诊断的精准性与效率。基层医疗机构由于缺乏专业的影像诊断医生，大量影像检查需要转诊至上级医院，患者等待时间长、就医成本高。通过 5G 网络，基层医疗机构可将 CT、MRI 等超高清医学影像实时上传至上级医院影像诊断中心，上级医院医生通过专业终端实时查看影像，进行精准诊断并出具报告，诊断结果实时反馈至基层医疗机构，整个过程仅需数分钟。相较于传统的影像传输方式，5G 技术实现了影像的无损传输，避免了压缩失真导致的诊断误差，同时大幅缩短了传输与诊断时间。某基层医院试点 5G 远程影像诊断后，患者影像诊断等待时间从平均 24 小时缩短至 30 分钟，转诊率降低 60%，有效提升了基层医疗服务能力。此外，5G 技术还支持多模态影像的同步传输与融合分析，医生可同时查看患者的 CT、MRI、PET-CT 等多种影像，提升诊断的全面性与准确性。

（二）5G+AI 辅助影像诊断协同应用

5G 技术与 AI 技术的协同融合，构建了远程影像诊断的智能化体系，提升了诊断效率与精准度。在这一应用模式中，基层医疗机构拍摄的医学影像经 5G 网络上传至云端 AI 诊断平台，AI 系统首先对影像进行初步筛查，识别疑似病灶并标注位置，再将标注后的影像与 AI 诊断建议同步传输至上级医院医生终端，医生基于 AI 标注进行最终诊断与确认。5G 网络的高带宽与低时延特性保障了影像

数据与 AI 分析结果的实时传输，边缘计算技术的融入则将 AI 分析任务部署在靠近基层医疗机构的边缘节点，进一步降低了数据传输 latency 与云端算力压力。某省部署的 5G+AI 远程影像诊断平台，针对肺结节、糖尿病视网膜病变等常见疾病的筛查准确率可达 95% 以上，上级医院医生的诊断效率提升 50% 以上。这种协同应用模式既发挥了 AI 技术的高效筛查优势，又保障了医生诊断的权威性，尤其适用于基层医疗机构的常见病、多发病筛查，推动了分级诊疗体系的落地。

三、5G+ 远程多学科会诊（MDT）：全维度精准协同

（一）超高清多终端实时协同会诊

5G 技术打破了传统远程多学科会诊的时空限制，构建了超高清多终端实时协同体系，实现了不同科室、不同地域专家的高效协同。在会诊过程中，患者的电子病历、医学影像、生命体征等数据通过 5G 网络实时共享至所有参会专家终端，专家通过 4K 超高清视频进行实时交流，可对影像进行放大、标注等操作，精准分享诊断意见。相较于传统的标清视频会诊，5G 超高清视频能够清晰呈现患者的细微体征（如皮肤颜色变化、肢体活动度），提升了会诊的直观性与准确性。某三甲医院通过 5G 技术开展远程多学科会诊，覆盖了全国 20 多个省份的基层医疗机构，会诊效率提升 50% 以上，疑难病例确诊时间从平均 7 天缩短至 2 天。此外，5G 技术还支持移动终端接入，专家可通过手机、平板等设备随时随地参与会诊，提升了会诊的灵活性与便捷性。

（二）5G+AR/VR 沉浸式远程会诊

5G 技术与 AR/VR 技术的融合，打造了沉浸式远程会诊场景，进一步提升了会诊的协同性与精准性。在 AR 远程会诊中，上级医院专家通过 AR 眼镜“虚拟查房”，可实时查看患者床头监护仪数据、触诊反馈（通过力反馈设备），并将诊断建议、影像标注等信息实时叠加在基层医生的视野中，实现“手把手”的远程指导。在 VR 远程会诊中，专家可通过 VR 设备进入虚拟诊疗空间，查看患者的三维影像模型，从不同角度观察病灶形态与周围组织的关系，为复杂病例的诊断提供更全面的空间信息。某医院试点 5G+AR 远程会诊后，基层医生对复杂病例的诊断准确率提升 40% 以上，上级专家的指导效率大幅提升。这种沉浸式会诊模式打破了传统平面化会诊的局限，为专家提供了更丰富的诊断信息，推动了远程会诊从“信息共享”向“深度协同”的升级。

四、5G+ 院前急救与远程监护：全周期精准保障

（一）院前急救与院内无缝协同应用

5G 技术构建了院前急救与院内诊疗的无缝协同体系，实现了“上车即入院”的精准急救模式。急救车上搭载 5G 高清摄像头、生命体征监测设备、移动超声等设备，能够将患者的实时视频、心电图、血压、血氧等数据通过 5G 网络实时回传至医院急诊科，同时传输现场外伤情况、患者意识状态等信息。医院急诊科医生基于这些实时数据，提前判断患者病情，启动相应的抢救预案，准备好所需药品、设备甚至手术团队，患者抵达医院后直接进入手术室或抢救室，大幅缩短了抢救准备时间。某急救中心统计，使用 5G 院前急救系统后，急性心梗患者的“门球时间”（从入院到球囊扩张的时间）从平均 90 分钟缩短至 60 分钟以内，抢救成功率提升 15%。此外，5G 技术还支持急救车与医院的实时视频连线，医院专家可通过视频指导急救人员进行现场急救操作，提升院前急救的规范性与有效性。

（二）慢性病远程精准监护应用

5G 技术与可穿戴设备的融合，构建了慢性病患者的远程精准监护体系，实现了从“院内治疗”到“院外管理”的全周期健康保障。高血压、糖尿病等慢性病患者佩戴搭载 5G 模块的智能手环、血压计、血糖仪等设备，能够实时采集生命体征数据，通过 5G 网络上传至云端健康管理平台。医生通过平台实时查看患者数据，当数据出现异常时，系统自动发出预警，医生及时与患者沟通，调整用药方案或安排复诊。同时，患者可通过移动端 APP 查看自身健康数据，接收医生的健康指导，提升自我管理能力。某社区医院试点 5G 远程慢性病监护后，高血压患者的血压控制达标率从 60% 提升至 85%，患者往返医院的次数减少 70%，既降低了患者的就医成本，又减轻了医院的诊疗压力。这种远程监护模式能够实现对慢性病患者的持续监测与精准管理，有效降低并发症发生率，提升患者生活质量。

第三节 5G 支持下的医疗设备泛在互联与高可靠数据传输

一、5G 驱动医疗设备泛在互联的技术架构与实现路径

（一）多层次医疗设备互联架构设计

5G 支持下的医疗设备泛在互联构建了“终端接入 - 网络传输 - 平台调度”的多层次架构，实现了院内各类医疗设备的全维度互联互通。在终端接入层，通过 5G 模组集成、5G 物联网网关适配等方式，完成传统医疗设备的智能化改造与新型智能设备的原生接入，覆盖诊断类设备（CT、MRI、超声仪）、治疗类设备（手术机器人、呼吸机、输液泵）、监护类设备（心电监护仪、血氧仪）及后勤管理类设备（药品配送机器人、环境监测传感器）等全品类医疗设备。针对不同设备的通信需求，采用差异化接入方案：对手术机器人等关键设备采用 5G 专网接入，保障低时延高可靠；对环境传感器等海量终端采用 5G 窄带物联网接入，降低功耗与成本。

在网络传输层，依托 5G 核心网切片技术，为医疗设备互联划分专属虚拟网络切片，实现设备数据与办公数据、患者服务数据的逻辑隔离，保障设备数据传输的安全性与专属带宽。通过 Massive MIMO、超密集组网等 5G 关键技术，提升室内外复杂医疗环境下的网络覆盖质量，解决手术室、ICU、地下影像中心等传统网络信号薄弱区域的设备接入难题。在平台调度层，构建 5G+ 医疗设备互联管理平台，集成设备注册、状态监测、数据汇聚、指令调度等核心功能，实现对全院互联设备的集中管控与协同调度，为设备间的数据交互与协同工作提供中枢支撑。

（二）传统医疗设备智能化改造路径

针对医院内大量传统医疗设备缺乏网络接口、无法直接互联的问题，5G 技术提供了低成本、高效率的智能化改造路径，推动存量设备的“互联升级”。一是模块化改造方案，通过外接 5G 通信模组（如工业级 5G DTU 模组），将传统医疗设备的 RS232/485 等串口数据转换为 5G 网络数据，实现数据的实时上传与远程控制，该方案无需改动设备核心结构，改造周期短、成本低，适用于超声仪、心电监护仪等中小体量设备。二是网关汇聚改造方案，对影像科、检验科等设备密集区域，采用 5G 物联网网关集中接入多台传统设备，通过网关完成数据采集、

协议转换与 5G 传输，大幅提升设备互联的规模化效率，适用于 CT、MRI、生化分析仪等大型设备集群。

三是边缘计算协同改造方案，在设备集中区域部署 5G 边缘计算节点，将设备数据的预处理、分析任务下沉至边缘端，减少核心网络传输压力，同时实现设备控制指令的本地快速响应，适用于对时延敏感的治疗类设备改造。某三甲医院通过上述改造方案，完成了全院 300 余台传统医疗设备的 5G 互联改造，设备数据接入效率提升 80%，实现了设备状态的实时监控与远程运维。

（三）新型智能医疗设备的 5G 原生互联实践

新一代智能医疗设备普遍采用 5G 原生设计，通过内置 5G 通信模块，实现与医院信息系统的无缝互联，大幅提升设备的协同工作能力与智能化水平。在诊断设备领域，5G 原生超声仪能够实时将超声影像传输至云端 AI 诊断平台，结合 AI 算法快速生成诊断建议，同时支持远程专家实时查看影像并进行指导；5G 原生移动 DR 设备可在床旁完成拍摄后，瞬间将影像数据上传至 PACS 系统，避免了传统设备的数据线连接与数据拷贝环节，提升床旁诊断效率。在治疗设备领域，5G 原生手术机器人通过专属网络切片实现与主操作端的低时延通信，支持多机器人协同手术，手术指令响应时延稳定在 10ms 以内；5G 原生输液泵能够实时上传输液速度、剩余药量等数据，当出现异常时自动报警并反馈至护士站，提升输液安全管理水平。

在监护设备领域，5G 原生可穿戴监护设备为重症患者、术后康复患者提供连续的生命体征监测，数据通过 5G 网络实时回传至监护中心，实现 24 小时不间断监护，尤其适用于康复期患者的院外管理。这些 5G 原生智能设备的应用，构建了“设备-人-系统”的全链路互联体系，推动医疗服务从“定点诊疗”向“全周期、全场景”服务转型。

二、5G 保障医疗数据高可靠传输的技术策略与实践价值

（一）医疗数据高可靠传输的技术保障体系

5G 技术通过多重技术策略构建了医疗数据高可靠传输保障体系，全面覆盖数据传输的完整性、实时性与安全性。在传输完整性保障方面，采用链路冗余备份技术，为关键医疗设备数据传输提供主备双链路，当主链路出现故障时，系统自动切换至备用链路，切换时延低于 50ms，确保数据传输不中断；通过前向纠

错编码（FEC）技术，对传输数据进行冗余编码处理，有效降低网络干扰导致的数据包丢失率，使医疗数据传输丢包率低于 0.001%。在传输实时性保障方面，依托 5G URLLC 特性，通过缩短传输时隙、优化调度算法，将医疗关键数据（如手术指令、生命体征数据）的端到端时延控制在 1-10ms，满足实时诊疗与设备控制需求；结合边缘计算技术，将数据处理节点部署在靠近设备的边缘端，减少数据传输路径长度，进一步降低传输时延。

在传输安全性保障方面，采用 5G 内生安全技术，对设备接入进行严格的身份认证与权限管理，防止非法设备接入；通过加密传输协议（如 IPSec VPN）对医疗数据进行全链路加密，确保数据在传输过程中不被窃取、篡改；利用网络切片技术实现医疗数据与其他数据的逻辑隔离，避免跨领域数据干扰与安全风险。某医院的 5G 医疗数据传输系统测试显示，在高网络负载情况下，生命体征数据传输时延稳定在 8ms 以内，丢包率为 0.0008%，完全满足临床诊疗的高可靠要求。

（二）不同类型医疗数据的差异化传输策略

针对医疗数据类型多样、传输需求差异显著的特点，5G 网络采用差异化传输策略，实现各类数据的精准适配。对于实时性、可靠性要求极高的关键医疗数据（如手术机器人控制指令、重症患者生命体征数据），采用高优先级网络切片，分配专属带宽与低时延传输资源，确保数据传输的实时响应与稳定可靠，同时启动链路冗余备份机制，应对突发网络故障。对于体量大、实时性要求中等的医疗数据（如医学影像、基因测序数据），采用大带宽网络切片，利用 5G eMBB 特性实现超高清影像、大容量数据的快速传输，同时采用数据压缩与分片传输技术，提升传输效率，减少网络资源占用。

对于实时性要求低、体量小的常规医疗数据（如患者基本信息、药品库存数据），采用通用网络切片，共享网络资源，降低传输成本，同时通过批量传输、非高峰时段传输等方式，优化网络资源利用效率。对于隐私敏感度极高的医疗数据（如患者基因数据、传染病诊疗记录），在采用加密传输的基础上，结合区块链技术实现数据传输全程可追溯，确保数据来源可查、去向可追，提升数据传输的安全性与可信度。这种差异化传输策略，既保障了关键医疗数据的传输质量，又实现了网络资源的高效利用，满足了医院多样化的数据传输需求。

（三）5G 高可靠数据传输的临床与管理实践价值

5G 保障的医疗数据高可靠传输，为临床诊疗与医院管理带来了多维度的实

践价值。在临床诊疗层面，实时、完整的医疗数据传输实现了诊疗决策的精准化与高效化。例如，重症监护场景中，患者的心率、血压、血氧等生命体征数据通过 5G 网络实时回传至监护中心，医生能够实时掌握患者病情变化，及时调整治疗方案，降低危重患者的死亡风险；多学科联合诊疗场景中，不同科室的诊疗数据、影像资料通过 5G 网络快速共享，专家能够基于完整的患者数据进行协同诊断，提升疑难病例的确诊效率。在医疗设备管理层面，设备运行数据的高可靠传输实现了设备的全生命周期管理，医院通过实时监测设备运行状态，能够提前预判设备故障，开展预防性维护，降低设备故障率与维修成本。

在医院运营管理层面，医疗数据的高效传输与汇聚为运营决策提供了精准的数据支撑。通过分析诊疗数据、设备使用数据、资源占用数据，医院能够优化科室排班、调整设备配置、合理分配医疗资源，提升运营效率。此外，5G 高可靠数据传输推动了远程医疗的规模化发展，使优质医疗资源能够跨区域高效辐射，为偏远地区患者提供精准诊疗服务，推动医疗资源的均衡配置。

第四节 5G 网络在突发公共卫生事件应急管理中的应用实践

一、突发公共卫生事件应急管理的 5G 网络架构与部署策略

（一）应急医疗 5G 网络架构设计

针对突发公共卫生事件(如传染病暴发、重大灾害医疗救援)的应急管理需求，5G 网络构建了“核心网 - 边缘网 - 接入网”三级应急架构，实现应急医疗场景的快速部署与高效通信。在核心网层面，采用虚拟化核心网技术，实现网络资源的弹性伸缩与快速部署，能够根据应急医疗队伍的规模与业务需求，动态调整核心网功能与资源配置；通过核心网切片技术，为应急医疗业务划分专属切片，保障应急数据传输的优先性与安全性。在边缘网层面，部署便携式 5G 边缘计算节点，将应急医疗数据的处理、分析任务下沉至边缘端，实现应急诊疗数据的本地快速处理与响应，减少核心网络传输压力，同时保障断网情况下的应急通信连续性。

在接入网层面，整合固定基站、移动基站（如车载基站、无人机基站）、卫星通信等多种接入方式，实现应急医疗场景的全域无缝覆盖。对于固定应急医疗点（如临时方舱医院），部署固定 5G 基站保障稳定通信；对于移动救援场景（如灾害现场救援），采用车载 5G 基站快速搭建临时通信网络；对于偏远地区或地

面网络中断场景，通过卫星-5G 融合通信实现应急数据的传输。这种三级应急架构具备快速部署、弹性伸缩、全域覆盖的特点，能够精准匹配突发公共卫生事件应急管理的动态需求。

（二）应急 5G 网络的快速部署与弹性扩容策略

突发公共卫生事件应急管理对网络部署的时效性要求极高，5G 网络通过“预制化、模块化、机动化”的部署策略，实现应急网络的快速搭建。一是预制化网络资源储备，运营商提前预制应急 5G 基站、边缘计算节点、核心网虚拟化模块等设备，当突发公共卫生事件发生时，可立即调运至应急现场，大幅缩短部署时间。二是模块化组网设计，将应急网络设备集成至标准集装箱或车载平台，形成可移动的“5G 应急通信车”“5G 应急方舱”，到达现场后通过简单拼接与调试即可完成网络部署，单套应急通信系统的部署时间可控制在 2 小时以内。三是机动化覆盖补充，针对复杂地形或地面网络无法覆盖的区域，采用无人机基站、系留气球基站等机动化设备，快速实现应急区域的网络覆盖，解决“最后一公里”通信难题。

同时，5G 网络具备弹性扩容能力，通过网络切片的动态调整与边缘计算资源的按需调度，能够根据应急医疗队伍的增减、诊疗业务的变化，实时扩展网络带宽与处理能力。例如，在大规模传染病暴发时，临时方舱医院的医疗设备、医护人员终端、患者服务终端数量激增，5G 网络可通过动态扩容将应急切片带宽从 100Mbps 提升至 1Gbps 以上，保障多终端、多业务的同时运行。某地区在应对突发传染病时，通过上述部署策略，仅用 1.5 小时就完成了临时方舱医院的 5G 网络全覆盖，支撑了 200 余台医疗设备、300 余部终端的同时接入，保障了应急诊疗工作的顺利开展。

二、5G 在突发公共卫生事件应急管理中的核心应用实践

（一）应急医疗现场与后方医院的实时协同诊疗

在突发公共卫生事件应急救援现场，5G 网络构建了应急医疗现场与后方核心医院的实时协同诊疗体系，实现了优质医疗资源的远程支撑。应急现场的医护人员通过 5G 高清视频终端、移动医疗设备，将患者的实时视频、生命体征数据、现场检查影像等信息实时传输至后方核心医院的专家团队，专家通过终端实时查看患者情况，进行远程会诊并制定治疗方案，指导现场医护人员开展救治工作。

5G 技术的低时延、高带宽特性保障了高清视频的流畅传输与医疗数据的实时交互，使远程会诊如同现场诊疗一样精准高效。^①

在大规模传染病应急场景中，临时方舱医院的患者诊疗数据通过 5G 网络实时同步至后方医院的信息系统，后方专家能够实时监控患者病情变化，及时调整治疗方案；对于重症患者，通过 5G 远程手术系统，后方专家可指导现场医生开展微创手术，提升重症患者的救治成功率。某突发传染病疫情中，某省通过 5G 构建的远程协同诊疗系统，实现了 10 家方舱医院与 5 家核心医院的实时联动，后方专家日均开展远程会诊 300 余例，指导现场救治重症患者 50 余例，有效提升了应急医疗救治能力。

（二）疫情监测与防控的数据实时采集与分析

5G 网络为突发传染病疫情的监测与防控提供了高效的数据采集与分析支撑，实现了疫情的精准防控。在数据采集层面，通过 5G 物联网技术接入社区、医院、交通枢纽等重点区域的体温监测设备、人员流动监测设备、环境消杀设备等，实时采集人员体温、流动轨迹、环境消杀状态等数据，形成全方位的疫情监测网络。这些数据通过 5G 网络快速上传至疫情防控指挥平台，实现疫情数据的实时汇聚。在数据分析层面，依托 5G 边缘计算与云端大数据分析技术，对汇聚的疫情数据进行实时分析，预测疫情发展趋势、识别高风险区域与人群，为疫情防控决策提供精准的数据支撑。

例如，在某城市疫情防控中，通过 5G 网络接入全市 2000 余个重点区域的监测设备，实时采集人员体温数据与流动信息，大数据分析平台基于这些数据快速识别出疫情传播链条，及时划定高风险区域并采取管控措施，有效遏制了疫情的扩散。此外，5G 技术还支持核酸检测数据的实时上传与共享，检测机构完成核酸检测后，数据通过 5G 网络立即同步至健康码平台与疫情防控指挥平台，实现核酸检测结果的快速查询与疫情数据的精准统计，提升疫情防控效率。

（三）应急医疗物资的全流程智能化管理

突发公共卫生事件应急管理中，医疗物资的快速调配与精准管理至关重要，5G 技术构建了应急医疗物资全流程智能化管理体系。在物资采购与运输环节，通过 5G 物联网技术为医疗物资（如口罩、防护服、药品、医疗器械）配备智能

^① 5G 技术全球首次用于灾难医学救援 中国移动与四川省人民医院联合开展 5G 应急医疗“高速”救援 [J]. 通信与信息技术, 2019, (04): 14.

标签,实时采集物资的位置、数量、温度、湿度等信息,通过 5G 网络上传至物资管理平台,实现物资运输过程的全程跟踪与监控;利用 5G+ 北斗定位技术,精准定位物资运输车辆,优化运输路线,确保物资快速送达应急现场。在物资存储与分发环节,应急医疗物资仓库通过 5G 网络接入智能货架、温湿度传感器、自动分拣设备等,实现物资存储环境的实时监测与物资的自动化分拣、分发;医护人员通过 5G 终端快速查询物资库存信息,提交领用申请,实现物资的精准领用与管理。

某地区在应对突发灾害医疗救援时,通过 5G 构建的应急医疗物资管理系统,实现了对 200 余种、10 万余件医疗物资的全流程管理,物资运输跟踪精度提升至 10 米以内,物资分发效率提升 60%,确保了救援现场医疗物资的及时供应。此外,5G 技术还支持跨区域物资调度协同,通过物资管理平台的全国联网,实现不同地区应急医疗物资的统筹调配,提升物资利用效率。

(四) 应急医疗队伍的远程培训与指挥调度

5G 网络为应急医疗队伍的远程培训与指挥调度提供了高效支撑,提升了应急医疗队伍的作战能力。在远程培训层面,针对突发公共卫生事件的诊疗规范、防护要求、设备操作等内容,通过 5G 超高清视频直播、VR 沉浸式培训等方式,对一线应急医疗人员开展实时培训;培训过程中,学员可通过 5G 终端与专家实时互动,提问答疑,快速掌握应急诊疗技能。在指挥调度层面,构建 5G 应急指挥调度平台,实现对分散在不同应急现场的医疗队伍的集中调度与统一管理;通过 5G 高清视频会议系统,指挥中心能够实时查看各应急现场的情况,与一线医护人员实时沟通,下达调度指令;利用 5G+GIS 技术,实现应急医疗队伍、医疗设备、物资的可视化管理,优化资源配置,提升指挥调度效率。

某省在疫情防控期间,通过 5G 远程培训系统为全省 2 万余名一线医护人员开展了 100 余场应急诊疗培训,培训覆盖效率提升 80%;通过 5G 应急指挥调度平台,实现了对 30 支应急医疗队伍的集中调度,及时调配医疗资源与人员支援重点区域,有效提升了疫情防控的整体协同能力。

三、5G 应急医疗应用的挑战与优化建议

(一) 当前应用面临的核心挑战

尽管 5G 在突发公共卫生事件应急管理中展现出显著优势,但当前应用仍面

临诸多挑战。一是应急网络部署的复杂性，突发公共卫生事件现场往往环境复杂（如灾害现场、偏远地区），地形、气候等因素会影响 5G 基站的部署与信号覆盖，导致网络部署难度增加；部分应急场景下电力供应不稳定，影响应急网络设备的持续运行。二是跨部门数据共享壁垒，应急医疗数据涉及卫生健康、公安、交通、运营商等多个部门，不同部门的数据标准不统一、共享机制不完善，导致数据无法有效汇聚与协同分析，影响应急决策效率。三是应急设备与技术的适配性不足，部分应急医疗设备缺乏 5G 适配能力，无法直接接入应急网络；现有 5G 应急技术方案在极端环境下的稳定性与可靠性仍需提升。四是专业人才短缺，既掌握 5G 通信技术又熟悉应急医疗管理的复合型人才匮乏，影响应急 5G 网络的部署、运维与优化效率。

（二）优化建议与发展方向

针对上述挑战，提出以下优化建议与发展方向。一是提升应急网络的抗干扰与自适应能力，研发便携式、高抗干扰的 5G 应急通信设备，优化设备的防水、防尘、抗震性能，适配复杂应急环境；开发太阳能、蓄电池等多能源供电的应急网络设备，保障极端环境下的持续供电。二是建立跨部门数据共享机制，制定统一的应急医疗数据标准与接口规范，构建一体化应急数据共享平台，打破部门间的数据壁垒，实现数据的高效汇聚与协同分析；加强数据安全和隐私保护，明确数据共享的范围与权限，确保数据使用安全合规。三是推动应急医疗设备的 5G 智能化升级，鼓励设备厂商研发 5G 原生应急医疗设备，提升设备的网络适配能力；加强 5G 与应急医疗技术的融合创新，如 5G+AI、5G+VR/AR 在应急诊疗中的深度应用，提升应急医疗的智能化水平。四是加强复合型人才培养，建立通信企业与医疗机构的合作培训机制，开展 5G 通信技术与应急医疗管理的复合型培训，提升相关人员的专业能力；组建专业的应急 5G 技术服务团队，为突发公共卫生事件应急管理提供技术支撑。

第三章 物联网技术在医院信息化管理中的应用研究

第一节 物联网技术架构与医疗应用基础

一、物联网技术核心架构解析

（一）感知层：医疗数据采集的核心入口

感知层作为物联网技术架构的基础层级，承担着医疗场景下各类数据的实时采集功能，是实现医院信息化精准管理的核心入口。该层级通过部署各类传感器、射频识别（RFID）标签、生物识别设备等终端，实现对医疗环境、设备状态、患者体征、物资信息等多维度数据的全面感知。其中，RFID 标签分为有源与无源两种类型，无源标签凭借低成本、低功耗、易部署的优势，广泛应用于医疗物资标识与溯源；有源标签则因通信距离远、数据传输速率高的特点，适配大型医疗设备的状态监测。

生物传感设备是感知层的关键组成部分，包括心电传感器、血氧传感器、体温传感器等，能够实现对患者生命体征数据的无创、连续采集，为临床诊疗提供实时数据支撑。环境传感器则聚焦于医院手术室、ICU、药房等特殊区域，实时监测温度、湿度、洁净度、有害气体浓度等环境参数，保障诊疗环境安全。感知层终端设备具备小型化、智能化、低功耗的特点，能够适应医院复杂的诊疗环境，实现数据采集的自动化与精准化，为后续数据传输与分析奠定基础。

（二）网络传输层：数据交互的高效通道

网络传输层是连接感知层与应用层的关键纽带，负责将感知层采集的海量医疗数据高效、可靠地传输至应用层处理平台。该层级整合了多种通信技术，形成“有线+无线”协同的多元化传输网络，适配医院不同场景的通信需求。在有线传输方面，依托 F5G 全光网技术构建高速骨干网络，实现医院各科室、各区域之间的数据高速交互，尤其适用于大型医学影像、基因测序等大容量数据的传输，保障数据传输的稳定性与安全性。

在无线传输方面，融合了 5G、Wi-Fi 7、LoRa、蓝牙等多种技术：5G 技术凭借低时延、高带宽、广连接的特性，支撑远程手术机器人控制、移动监护等实时性要求高的场景；Wi-Fi 7 则广泛应用于门诊、病房等区域，满足医护人员移动终端、患者服务终端的高速接入需求；LoRa 技术因低功耗、长距离传输的优势，适配医院户外区域、地下库房等广覆盖场景的物联网设备接入；蓝牙技术则适用于短距离、小数据量的设备交互，如医疗设备与终端的近距离通信。网络传输层通过动态适配不同通信技术，实现了医疗数据传输的全方位覆盖与高效协同，保障数据在复杂医院环境下的实时交互。

（三）平台层：数据处理与资源调度的核心中枢

平台层是物联网技术在医院信息化管理中实现数据价值转化的核心中枢，集成了数据汇聚、存储、处理、分析、调度等多种功能，为上层应用提供标准化的数据服务与资源支撑。该层级主要包括物联网平台、数据中台、边缘计算节点三大核心组件：物联网平台负责对接感知层各类终端设备，实现设备的注册、管理、监控与指令下发，支持多种通信协议的解析与转换，保障不同类型设备的互联互通；数据中台则承担着医疗数据的汇聚、清洗、标准化处理任务，通过构建统一的数据模型，实现患者数据、设备数据、物资数据、环境数据的整合与管理，为数据分析提供高质量的数据基础。

边缘计算节点的部署是平台层的重要创新，将部分数据处理任务下沉至医院各区域边缘端，实现医疗数据的本地实时分析与响应，减少核心网络传输压力，提升数据处理效率。例如，在手术室部署边缘计算节点，可实时处理手术设备数据与患者生命体征数据，及时反馈异常信息，保障手术安全。平台层通过构建“云-边-端”协同的处理架构，实现了医疗数据的高效处理与资源的智能调度，为医院信息化管理的各类应用场景提供精准的数据支撑。

（四）应用层：场景化落地的价值输出载体

应用层是物联网技术与医院信息化管理场景深度融合的价值输出载体，基于平台层提供的数据服务，针对医院诊疗服务、设备管理、物资管理、环境管理等核心需求，构建多样化的场景化应用解决方案。在临床诊疗领域，形成了智能监护、远程诊疗、AI 辅助诊断等应用；在设备管理领域，打造了医疗设备全生命周期管理系统；在物资管理领域，构建了药品、耗材的溯源与库存管理系统；在环境管理领域，实现了医院特殊区域的环境参数实时监控与智能调控。

应用层具有模块化、可扩展的特点，医院可根据自身发展需求，灵活部署不同应用模块，并实现各模块之间的数据互通与协同联动。例如，医疗设备管理应用与物资管理应用可通过数据中台实现联动，当医疗设备需要维修时，自动触发耗材领用申请流程；智能监护应用与临床诊疗应用联动，可将患者实时体征数据同步至电子病历系统，辅助医生精准诊断。应用层的场景化落地，将物联网技术的技术优势转化为医院管理的实际效能，推动医院信息化管理向精准化、智能化方向转型。

二、物联网技术的医疗应用基础条件

（一）标准化体系支撑：打破设备与数据壁垒

标准化体系是物联网技术在医院信息化管理中规模化应用的基础前提，能够有效打破不同厂商设备之间、不同系统之间的互联互通壁垒。当前，医疗物联网领域的标准化建设主要聚焦于三个核心维度：一是设备接口标准化，通过制定统一的设备通信接口规范，实现不同品牌、不同类型医疗物联网设备的无缝对接，避免因接口不兼容导致的设备孤立问题；二是数据格式标准化，规范医疗数据的采集、存储、传输格式，确保患者体征数据、设备运行数据、物资信息等各类数据的一致性与可解读性，为数据整合与分析提供保障；三是应用协议标准化，统一物联网设备与平台、平台与应用之间的通信协议，提升数据传输的效率与可靠性。

国内已出台多项医疗物联网相关标准，其为医院物联网建设提供了技术遵循。同时，行业内正推动医院信息系统与物联网平台的标准化对接，实现物联网数据与电子病历（EMR）、医院信息管理系统（HIS）、医学影像信息系统（PACS）等核心系统的数据互通，构建一体化的医院信息管理体系。标准化体系的不断完善，为物联网技术在医院的深度应用奠定了坚实基础。

（二）安全防护体系：保障医疗数据与设备安全

医疗数据的敏感性与医疗设备的安全性决定了安全防护体系是物联网技术在医院应用的核心保障。医院物联网安全防护体系覆盖“终端-网络-平台-应用”全链路，构建了多层次的安全防护机制。在终端安全层面，对物联网终端设备进行严格的身份认证与权限管理，采用加密芯片、安全固件等技术，防止设备被非法入侵与控制；对无源RFID标签等低成本终端，通过数据加密、访问控制等方式，保障标签信息不被窃取与篡改。

在网络安全层面,采用网络隔离、防火墙、入侵检测与防御系统等技术,实现物联网网络与医院核心业务网络的逻辑隔离,防止网络攻击扩散;对数据传输过程采用 SSL/TLS 等加密协议,确保数据在传输过程中的安全性与完整性。在平台与应用安全层面,构建数据安全审计系统,对数据的采集、存储、使用、传输全流程进行监控与审计,及时发现并处置数据安全风险;采用访问控制、数据脱敏等技术,保障医疗数据的隐私安全。此外,建立常态化的安全应急响应机制,定期开展安全演练,提升应对网络攻击、数据泄露等安全事件的处置能力,为物联网技术在医院的安全应用保驾护航。

(三) 基础设施支撑: 构建全场景覆盖网络

完善的基础设施是物联网技术在医院信息化管理中落地应用的重要保障,主要包括网络基础设施与硬件部署环境两部分。在网络基础设施方面,医院需构建“全光网+无线网络”协同覆盖的网络架构:通过 F5G 全光网实现医院各区域的有线网络全覆盖,保障大容量医疗数据的高速传输;部署 5G、Wi-Fi 6 等无线网络,实现门诊、病房、手术室、库房等全场景的无线覆盖,满足物联网终端设备的移动接入需求。同时,部署边缘计算节点,优化数据处理路径,提升数据处理效率。

在硬件部署环境方面,需根据医院不同场景的需求,合理规划物联网终端设备的部署位置与数量:在病房区域部署患者监护传感器、床头呼叫终端等设备;在手术室部署手术设备状态监测终端、环境参数传感器等;在药房、库房部署 RFID 读写器、物资监测传感器等。此外,构建标准化的设备安装与运维环境,保障物联网设备的稳定运行。随着医院数字化转型的推进,越来越多的医院加大了基础设施投入,为物联网技术的规模化应用提供了坚实的硬件支撑。

(四) 人才与运维体系: 保障技术持续高效应用

专业的人才队伍与完善的运维体系是保障物联网技术在医院持续高效应用的关键。物联网技术在医院的应用涉及物联网技术、医疗业务、信息管理等多个领域,需要具备跨学科知识的复合型人才进行规划、部署与运维。医院需组建专业的物联网技术团队,负责设备选型、网络部署、平台搭建、应用开发等工作;同时,加强对医护人员、管理人员的培训,提升其对物联网设备与应用系统的使用能力。

在运维体系方面,构建“智能化监测+专业化运维”的协同体系:通过物联网平台实现对终端设备、网络状态、数据传输的实时监测,及时发现设备故障与

网络异常；建立标准化的运维流程，明确运维责任分工，确保故障快速响应与修复；引入第三方专业运维服务，提升运维效率与专业化水平。完善的人才与运维体系，能够有效解决物联网技术应用过程中的技术难题，保障系统的稳定运行，充分发挥物联网技术在医院信息化管理中的价值。

第二节 智能医疗设备全生命周期管理与物资溯源闭环管理

一、智能医疗设备全生命周期管理体系构建与应用

（一）设备准入与初始化管理：筑牢全生命周期起点

设备准入与初始化管理是智能医疗设备全生命周期管理的起点，通过物联网技术实现设备准入的标准化、初始化的自动化，为后续管理奠定基础。在设备准入阶段，构建基于物联网平台的准入审核系统，对拟采购的医疗设备进行技术参数校验、兼容性测试、安全评估，确保设备符合医院信息化管理要求。通过接入设备厂商的产品数据库，自动获取设备型号、技术参数、认证证书等信息，实现准入审核的高效化与精准化，避免因设备不兼容、不安全导致的应用风险。

在设备初始化阶段，为每台设备分配唯一的 RFID 标识，将设备基本信息（型号、规格、生产厂家、采购时间、质保期等）写入 RFID 标签，并录入物联网管理平台，建立设备电子档案。通过物联网技术实现设备与医院信息系统的自动对接，完成设备网络配置、权限设置、数据接口调试等初始化工作，确保设备能够快速接入医院物联网网络，实现数据的实时采集与传输。某三甲医院通过物联网技术实现医疗设备准入与初始化管理后，设备准入审核时间从平均 7 天缩短至 2 天，初始化部署效率提升 60%。

（二）设备运行状态实时监测与预警：保障诊疗安全

基于物联网技术的设备运行状态实时监测与预警，是保障医疗设备安全、稳定运行的核心环节。通过在医疗设备上部署振动传感器、温度传感器、电流传感器等状态监测终端，实时采集设备运行参数（如运行温度、振动频率、工作电流、运行时长等），并通过物联网网络传输至管理平台。平台通过构建设备运行状态评估模型，对采集的参数进行实时分析，判断设备运行状态是否正常。

当设备运行参数超出正常阈值时，系统自动发出预警信息，通过短信、APP

推送等方式通知运维人员与使用科室，同时在平台上标注设备位置与故障类型，指导运维人员快速处置。对于关键医疗设备（如手术机器人、呼吸机、监护仪等），采用 5G 低时延网络实现运行状态的毫秒级监测与预警，确保设备故障能够及时发现与处理，避免因设备故障影响诊疗工作。

（三）设备维护与维修管理：实现预防性维护

物联网技术推动医疗设备维护与维修管理从“事后维修”向“预防性维护”转型，大幅提升维护效率，降低维护成本。物联网管理平台根据设备运行数据、使用频率、质保期等信息，自动生成个性化的预防性维护计划，明确维护时间、维护内容、维护人员，通过平台推送至运维人员终端。运维人员按照维护计划开展维护工作，完成后在平台上记录维护情况，更新设备维护档案。

当设备出现故障时，使用科室可通过物联网终端快速提交维修申请，平台自动分配维修任务至对应运维人员，并提供设备故障信息、历史维修记录等数据支撑，辅助运维人员精准定位故障原因，提升维修效率。对于无法现场修复的故障，平台自动对接设备厂商的远程维修系统，通过物联网技术实现设备故障的远程诊断与指导，缩短维修周期。

（四）设备盘点与报废处置：实现全周期闭环管理

物联网技术实现了医疗设备盘点与报废处置的自动化、精准化，构建了全生命周期闭环管理。在设备盘点阶段，运维人员通过手持 RFID 读写器扫描设备标签，快速获取设备信息，实现设备的快速盘点。物联网平台实时同步盘点数据，自动对比盘点结果与设备档案，生成盘点报告，标注缺失、错位的设备，大幅提升盘点效率与准确性。传统人工盘点方式平均需要 3-5 天完成全院设备盘点，采用物联网技术后，盘点时间可缩短至 1 天以内，盘点准确率提升至 99.9%。

在设备报废处置阶段，物联网平台根据设备使用年限、故障率、维修成本等数据，自动生成设备报废建议。经审核通过后，系统更新设备状态为“报废”，并记录报废时间、处置方式等信息。通过 RFID 标签跟踪设备报废后的处置流程，确保报废设备得到规范处理，避免医疗废物污染与信息泄露。同时，平台对报废设备的相关数据进行统计分析，为后续设备采购提供数据支撑，优化设备配置方案。

二、医疗物资溯源闭环管理体系构建与应用

（一）物资采购与入库溯源：筑牢源头管控

医疗物资采购与入库溯源是物资溯源闭环管理的源头，通过物联网技术实现采购过程的透明化、入库管理的精准化。在采购阶段，医院物联网平台与供应商管理系统对接，实现采购订单的在线生成、审核与跟踪。为每批采购物资分配唯一的 RFID 溯源标签，标签关联物资名称、规格、生产厂家、生产日期、有效期、批次、供应商等全链条信息，实现物资采购信息的全程可追溯。

在入库阶段，库房工作人员通过 RFID 读写器扫描物资标签，自动采集物资信息，与采购订单进行比对，确认无误后完成入库登记，系统自动更新库存数据。对于需要特殊存储条件的物资（如药品、血液制品），物联网系统实时监测库房温度、湿度等环境参数，确保物资存储安全。入库完成后，系统生成入库报告，同步至医院财务系统与物资管理系统，实现采购、入库、财务结算的协同联动。某医院通过物联网技术实现医疗物资采购与入库溯源后，入库审核时间缩短 70%，采购物资差错率降低 80%，有效筑牢了物资管理的源头管控。^①

（二）物资存储与库存动态管理：优化库存配置

基于物联网技术的物资存储与库存动态管理，实现了医疗物资库存的精准化、智能化管控，避免库存积压与短缺。在存储阶段，通过在库房部署智能货架、温湿度传感器、RFID 读写器等设备，实时监测物资存储状态与环境参数。智能货架能够自动识别物资位置与数量，当物资被取走或补充时，系统自动更新库存数据；温湿度传感器实时采集库房环境数据，当参数超出阈值时，自动触发预警并启动调控设备（如空调、除湿机），保障物资存储质量。

在库存管理阶段，物联网平台根据物资消耗速率、有效期、安全库存阈值等数据，自动生成库存预警信息：当物资库存低于安全阈值时，系统自动触发采购申请；当物资临近有效期时，系统发出效期预警，优先推送至使用科室领用。通过大数据分析技术，平台对物资消耗数据进行统计分析，预测物资需求趋势，优化库存配置方案，降低库存积压成本。某医院通过物联网技术实现物资库存动态管理后，库存积压金额减少 30%，物资短缺率降低 90%，库存周转率提升 40%。

① 欧吕平. 物联网技术下医院信息化管理系统的应用研究 [J]. 信息与电脑, 2025, 37 (01): 80-82.

（三）物资领用与使用追踪：实现全程溯源

物联网技术实现了医疗物资领用与使用的全程追踪，确保物资流向清晰、可追溯。在领用阶段，使用科室通过物联网终端提交领用申请，经审核通过后，库房工作人员根据申请信息快速定位物资位置，通过 RFID 读写器完成物资领用登记，系统自动更新库存数据。对于高值耗材（如人工关节、心脏支架），采用一对一的 RFID 标签标识，领用过程中关联患者信息，实现“物资-患者”的精准绑定。

在使用阶段，通过物联网技术跟踪物资使用情况，记录使用时间、使用人员、使用患者、使用科室等信息，实时同步至物资管理平台与电子病历系统。对于未使用的物资，如需退回库房，系统通过 RFID 标签识别物资信息，完成退回登记并更新库存。这种全程追踪模式，能够有效避免物资流失与滥用，同时在发生医疗纠纷或物资质量问题时，可快速追溯物资全链条信息，明确责任。某医院通过物联网技术实现高值耗材全程溯源后，耗材流失率降低 95%，质量问题追溯时间从平均 3 天缩短至 2 小时。

（四）物资报废与回收处置：闭环管理收尾

医疗物资报废与回收处置是溯源闭环管理的最后环节，通过物联网技术实现报废物资的规范处置与全程追踪。对于过期、损坏、不合格的医疗物资，使用科室或库房通过物联网平台提交报废申请，注明报废原因、数量、处置方式等信息，经审核通过后，系统更新物资状态为“报废”，并生成报废清单。报废物资在处置前，通过 RFID 标签进行标识，确保报废物资与清单一致。

在回收处置阶段，通过物联网技术跟踪报废物资的运输、销毁过程，记录处置单位、处置时间、处置方式等信息，确保报废物资得到规范处理，符合环保与医疗废物管理要求。对于可回收利用的物资（如废旧医疗设备零部件），系统通过 RFID 标签跟踪回收、修复、再利用过程，实现资源的循环利用。处置完成后，系统生成报废处置报告，同步至相关管理部门，实现报废处置的全流程闭环管理。某医院通过物联网技术实现医疗物资报废与回收处置后，报废物资处置效率提升 60%，处置合规率达到 100%，有效降低了环境与安全风险。

三、物联网技术在设备与物资管理中的应用价值与成效

（一）提升管理效率，降低运营成本

物联网技术的应用大幅提升了医院设备与物资管理的自动化水平，减少了人

工干预，提升了管理效率。在设备管理方面，自动化的状态监测、预防性维护与快速盘点，减少了运维人员的人工工作量，提升了设备利用效率；在物资管理方面，自动化的入库、盘点、库存预警与溯源追踪，缩短了物资流转时间，降低了库存积压与短缺风险。某医院应用物联网技术后，设备与物资管理相关岗位人员工作量减少 40%，管理流程平均耗时缩短 50%，运营成本降低 25%，实现了管理效率与经济效益的双重提升。

（二）保障诊疗安全，提升医疗质量

智能医疗设备的实时监测与预警，能够及时发现设备故障，避免因设备问题导致的诊疗差错；医疗物资的全程溯源，确保了物资质量，避免不合格物资用于临床诊疗。同时，设备与物资管理数据的精准采集与分析，为医院质量管理提供了数据支撑，有助于优化诊疗流程，提升医疗质量。某医院应用物联网技术后，因设备故障导致的诊疗差错率降低 60%，因物资质量问题引发的医疗纠纷减少 80%，医疗质量评分提升 15%，有效保障了患者诊疗安全。

（三）优化资源配置，提升服务能力

通过对设备运行数据、物资消耗数据的大数据分析，医院能够精准掌握资源使用情况，优化设备与物资配置方案，提升资源利用效率。例如，根据不同科室的设备使用频率，合理调配设备资源，避免部分科室设备闲置、部分科室设备短缺的问题；根据物资需求趋势，优化采购与库存方案，确保物资及时供应。资源配置的优化，有效提升了医院的诊疗服务能力，缩短了患者就医等待时间，改善了患者就医体验。某医院应用物联网技术后，设备资源利用率提升 30%，患者平均就医等待时间缩短 20%，患者满意度提升 25%。

（四）实现数据驱动，推动管理升级

物联网技术实现了设备与物资管理数据的全面采集与整合，构建了数据驱动的管理模式。通过对管理数据的深度分析，能够发现管理过程中的问题与薄弱环节，为管理决策提供精准的数据支撑。同时，数据的共享与协同，推动了医院各部门之间的协同联动，打破了管理壁垒，实现了医院信息化管理的一体化升级。物联网技术的应用，不仅提升了设备与物资管理的精细化水平，更推动了医院整体管理模式创新与转型，为智慧医院建设奠定了坚实基础。

第三节 物联网赋能的多维度患者监护与院内外健康协同管理

一、院内多维度患者监护体系构建与应用

（一）重症患者多体征实时精准监护

物联网技术构建了重症患者多体征实时精准监护体系，通过整合多类型传感设备与智能终端，实现对重症患者生命体征的全面、连续、精准监测，为临床诊疗提供可靠数据支撑。在 ICU、重症病房等核心区域，为患者配备集成心电图、血氧、血压、体温、呼吸频率等多参数的可穿戴监护设备，设备通过物联网网络（5G/Wi-Fi 6）将实时采集的体征数据传输至中央监护平台，平台对数据进行实时解析与动态展示。

针对重症患者的特殊需求，系统构建设备联动与智能预警机制：当患者某一体征参数超出安全阈值时，平台立即触发多级预警，通过声光报警、终端推送等方式同步通知医护人员，同时自动关联患者电子病历、诊疗方案等信息，辅助医护人员快速判断病情。此外，监护设备可与呼吸机、输液泵等治疗设备实现联动，当患者体征出现异常波动时，系统自动提示医护人员调整治疗参数，甚至触发设备的应急调控逻辑（如紧急提升氧浓度）。某三甲医院 ICU 应用该体系后，重症患者体征异常发现时间缩短至 30 秒内，应急处置响应效率提升 50%，重症患者救治成功率提升 12%。^①

（二）术后患者康复状态动态监护

物联网技术为术后患者康复状态监护提供了智能化解决方案，实现从“被动巡查”到“主动监测”的转型，提升康复管理的精准性与效率。术后患者佩戴轻量化可穿戴监护设备，实时采集心率、血压、伤口压力、活动量等关键康复指标，数据通过物联网网络传输至康复管理平台。平台根据患者手术类型、病情特点构建个性化康复评估模型，对采集的数据进行动态分析，判断患者康复进展。

当出现异常指标（如伤口压力异常升高提示出血风险、活动量不足影响康复）时，系统自动发出预警，医护人员及时介入干预；同时，平台根据康复数据自动生成个性化康复指导方案，通过移动端 APP 推送至患者及家属，包括活动强度、饮食建议、伤口护理要点等。某医院针对骨科术后患者部署该系统后，术后并发症发生

① 赵艳，宋平，朱立峰. 基于物联网的医疗设备信息化平台建设实践 [J]. 中国数字医学, 2024, 19 (03): 68-73.

率降低 35%，患者康复周期缩短 20%，医护人员术后巡查工作量减少 40%。

（三）特殊患者定位与安全监护

针对老年痴呆、精神疾病、儿童等特殊患者的安全管理需求，物联网技术构建了精准定位与安全监护体系，有效降低患者走失、跌倒等安全风险。通过在患者佩戴的腕带、胸牌中集成 RFID 或 UWB 定位模块，在医院各区域部署定位基站，实现对患者的实时精准定位，定位精度可达 1-3 米。

系统支持电子围栏功能，医护人员可根据患者病情设置安全活动区域，当患者超出设定区域时，系统立即触发声光预警，并将患者实时位置推送至医护人员终端；同时，定位终端集成跌倒检测、一键呼救等功能，患者发生跌倒或突发不适时，可通过终端快速呼救，系统自动锁定患者位置并通知医护人员。某医院老年病科应用该体系后，患者走失率降至 0，跌倒事件发生率降低 65%，患者家属满意度提升 30%。

二、院内外健康协同管理体系构建与应用

（一）慢性病患者院外远程监护与管理

物联网技术打破了医院边界，构建了慢性病患者院外远程监护与管理体系统，实现高血压、糖尿病、冠心病等慢性病患者的全周期健康管理。患者在院外佩戴集成物联网模块的智能血压计、血糖仪、心电贴等设备，实时采集血压、血糖、心率等关键健康数据，通过 5G 或 LoRa 网络传输至医院慢性病管理平台。

平台对患者健康数据进行实时监测与趋势分析，当数据出现异常时（如血压骤升、血糖超标），系统自动发出预警，医护人员及时通过电话、APP 等方式与患者沟通，调整用药方案或安排复诊；同时，平台为患者提供个性化健康管理服务，包括用药提醒、饮食指导、运动建议等，患者可通过 APP 查询健康数据、提交咨询问题，实现与医护人员的高效互动。某社区医院应用该体系后，辖区内慢性病患者血压控制达标率从 62% 提升至 85%，急诊就诊率降低 40%，住院率降低 25%。

（二）康复期患者院外延续性护理管理

物联网技术实现了康复期患者院外延续性护理管理，确保患者出院后能够获得持续、规范的康复指导与护理服务，提升康复效果。患者出院时配备便携式康复监护设备与智能护理终端，院外实时采集康复训练数据（如关节活动度、训练

强度、完成度)、伤口愈合状态(通过智能摄像头采集图像)等信息,通过物联网网络传输至医院康复护理平台。^①

医护人员通过平台实时查看患者康复进展,根据康复数据调整康复训练方案,通过视频指导、语音留言等方式为患者提供远程护理指导;对于需要定期换药、复查的患者,平台自动生成提醒,确保患者按时完成相关护理流程。同时,患者可通过终端上传康复过程中遇到的问题,医护人员及时给予解答。某医院针对脑卒中康复期患者部署该系统后,患者院外康复依从性提升 70%,康复效果评分提升 18%,二次入院率降低 32%。

(三) 院内外健康数据协同与诊疗闭环构建

物联网技术推动了院内外健康数据的协同整合,构建了“院内诊疗-院外管理-院内复诊”的诊疗闭环。通过打通院内外健康管理平台与医院核心信息系统(EMR、HIS、PACS),实现患者院内外健康数据的无缝对接与共享:患者院外监测的健康数据自动同步至电子病历系统,为复诊时医生的诊疗决策提供完整数据支撑;医生根据患者院外健康状况调整诊疗方案,方案实时同步至院外健康管理平台,指导患者院外健康管理。

同时,系统构建智能转诊机制,当院外患者出现紧急健康状况时,平台自动将患者院外健康数据、历史诊疗记录同步至急诊科,协助急诊科医生快速掌握病情,提升应急处置效率。某医院通过该协同体系,实现了心血管疾病患者的全周期管理,患者复诊时医生诊疗决策时间缩短 40%,应急处置响应时间缩短 35%,诊疗连续性与精准性大幅提升。

三、物联网赋能患者监护与健康协同的技术支撑与保障

(一) 轻量化、低功耗传感设备技术支撑

轻量化、低功耗传感设备是物联网赋能患者监护的核心硬件支撑,技术的不断升级为患者提供了更舒适、更持久的监测体验。通过采用柔性电子、微机电系统(MEMS)等先进技术,监护设备实现了小型化、轻量化设计,如贴片式心电传感器、柔性血氧腕带等,减少了对患者活动的限制;低功耗芯片与节能通信协议的应用,大幅提升了设备续航能力,部分可穿戴设备续航时间可达 7-14 天,

① 陶皓. 基于物联网技术的智慧医院系统设计[J]. 数字通信世界, 2023, (04): 83-85.

避免了频繁充电对患者的困扰。

同时,传感设备的精准度不断提升,通过多传感器融合技术,有效降低了运动干扰、环境干扰对监测数据的影响,确保数据采集的准确性。例如,抗干扰血糖传感器能够有效避免饮食、运动对血糖监测结果的影响,监测误差控制在 5% 以内。这些技术突破,为院内外患者监护的规模化应用提供了硬件保障。

（二）健康数据安全与隐私保护保障

患者健康数据的敏感性决定了安全与隐私保护是物联网赋能健康管理的核心保障。通过构建“终端-网络-平台”全链路安全防护体系,确保健康数据的安全可控。在终端层面,对采集的健康数据进行本地加密存储,采用设备身份认证技术,防止设备被非法入侵与数据篡改;在网络层面,采用 SSL/TLS 加密传输协议,实现健康数据的加密传输,避免数据在传输过程中被窃取。

在平台层面,构建数据访问权限管理体系,严格控制不同角色对健康数据的访问权限,采用数据脱敏技术对患者个人身份信息进行处理,避免隐私泄露;同时,建立数据安全审计系统,对数据的采集、存储、使用、传输全流程进行监控与审计,及时发现并处置安全风险。此外,严格遵循《个人信息保护法》《医疗机构病历管理规定》等法律法规,明确数据使用边界,确保健康数据管理的合规性。

（三）智能算法与数据挖掘技术赋能

智能算法与数据挖掘技术为健康数据的价值转化提供了核心支撑,实现了从“数据采集”到“智能分析”的升级。通过构建机器学习、深度学习等智能算法模型,对海量院内外健康数据进行分析,实现病情预警、康复评估、风险预测等功能。例如,基于 LSTM 神经网络的慢性病病情预警模型,能够通过分析患者历史健康数据,预测病情恶化风险,提前 3-7 天发出预警;基于随机森林算法的康复评估模型,能够根据患者康复训练数据,精准评估康复效果,为调整康复方案提供数据支撑。

同时,通过数据挖掘技术,能够从群体健康数据中挖掘疾病发病规律、危险因素等信息,为医院的健康管理策略制定、公共卫生决策提供数据支撑。智能算法与数据挖掘技术的应用,大幅提升了院内外健康管理的智能化水平,推动了健康管理从“经验驱动”向“数据驱动”转型。

第四节 物联网在医院环境智能监控与预警中的应用

一、医院核心区域环境智能监控系统构建

（一）手术室环境全参数精准监控

手术室作为医院核心诊疗区域，对环境参数有着极高的要求，物联网技术构建了手术室环境全参数精准监控体系，保障手术安全与质量。通过在手术室部署温湿度传感器、洁净度传感器、压差传感器、有害气体传感器（如甲醛、臭氧）、微生物传感器等多类型传感设备，实时采集手术室温度、湿度、洁净度（含尘浓度）、压差、有害气体浓度、微生物数量等关键环境参数。

采集的数据通过物联网网络传输至环境管理平台，平台对数据进行实时解析与动态展示，确保各项参数符合《医院洁净手术部建筑技术规范》要求（如温度控制在 22-25℃、相对湿度 40%-60%、洁净度百级手术间含尘浓度 ≤ 350 粒/m³）。当某一参数超出阈值时，系统立即触发声光预警，并自动联动空调、新风系统、净化系统等设备进行调控，确保环境参数快速恢复正常。某医院通过该体系实现手术室环境监控后，环境参数达标率从 92% 提升至 99.5%，因环境问题导致的手术感染率降低 45%。

（二）ICU 与新生儿科环境精细化监控

ICU 与新生儿科患者免疫力低下，对环境质量要求严苛，物联网技术实现了该类区域环境的精细化监控与智能调控。在 ICU 区域，除常规温湿度、洁净度监控外，重点部署细菌、病毒等微生物传感器，实时监测空气中有害微生物浓度，同时监测室内噪声、光照强度等参数，为患者营造安静、舒适的诊疗环境；在新生儿科，针对早产儿、低体重儿的特殊需求，部署高精度温湿度传感器，将温度控制精度提升至 $\pm 0.5^{\circ}\text{C}$ ，湿度控制精度 $\pm 3\%$ ，同时监测室内 CO₂ 浓度，确保空气质量。

环境管理平台对采集的参数进行实时分析，当出现异常时（如微生物浓度超标、温湿度波动），立即发出预警并联动相关设备进行调控；同时，系统自动记录环境参数变化曲线，形成环境管理档案，为医院感染控制、质量追溯提供数据支撑。某医院新生儿科应用该体系后，新生儿感染发生率降低 50%，患者家属满意度提升 28%。

（三）药房与试剂库房环境专项监控

药房与试剂库房存储的药品、试剂对存储环境有着严格要求，物联网技术构建了该类区域环境专项监控体系，保障药品与试剂质量。通过在药房、试剂库房部署高精度温湿度传感器、冷链监测传感器、光照传感器、气体传感器等设备，实时采集存储环境参数：常温药房温度控制在 0-30℃，阴凉药房温度 $\leq 20^{\circ}\text{C}$ ，冷藏药房 / 试剂库房温度控制在 2-8℃，相对湿度控制在 35%-75%；同时监测是否存在有害气体、光照强度是否超标等。

对于冷链存储的药品与试剂，通过在冷藏柜、冷藏车中部署冷链监测终端，实现全程温度监控，数据实时传输至环境管理平台，当温度超出阈值时，系统立即触发多级预警，通知库房管理人员及时处置；同时，系统自动记录冷链温度变化曲线，形成全程可追溯的冷链管理档案。某医院通过该体系实现药房与试剂库房环境监控后，药品变质损耗率降低 80%，试剂质量合格率提升至 100%，有效保障了用药安全。

二、医院公共区域环境智能监控与管理

（一）门诊与住院楼公共区域环境监控

门诊与住院楼公共区域人员密集，环境质量直接影响患者就医体验与健康，物联网技术实现了该类区域环境的智能监控与优化。通过在大厅、走廊、电梯间等公共区域部署温湿度传感器、PM2.5 传感器、CO₂ 传感器、噪声传感器等设备，实时采集环境参数，数据传输至环境管理平台。平台对数据进行实时分析，当 PM2.5 浓度超标、CO₂ 浓度过高（ $\geq 1000\text{ppm}$ ）、噪声过大（ $\geq 60\text{dB}$ ）时，系统自动联动新风系统、空气净化设备、电梯通风设备等进行调控，改善公共区域空气质量与舒适度。

同时，系统根据不同时段人员流量变化，动态调整环境调控设备的运行参数，在保障环境质量的同时降低能耗。例如，门诊高峰时段（上午 8-12 点）自动提升新风系统运行功率，非高峰时段降低运行功率。某医院应用该体系后，公共区域 PM2.5 达标率提升至 98%，CO₂ 浓度稳定在 800ppm 以下，患者就医环境满意度提升 32%。

（二）医院污水处理与医疗废物暂存环境监控

医院污水处理与医疗废物暂存环境的安全管理是医院环保与感染控制的重要

环节,物联网技术构建了该类区域环境专项监控体系,防范环境污染与感染风险。在污水处理站,部署 pH 值传感器、COD 传感器、氨氮传感器、溶解氧传感器等设备,实时监测污水处理过程中的关键参数,确保污水处理效果符合排放标准;同时监测污水处理站周边有害气体浓度(如硫化氢、氨气),避免气体泄漏造成环境污染。

在医疗废物暂存间,部署温湿度传感器、有害气体传感器、红外感应传感器等设备,实时监测暂存环境参数,确保医疗废物存储符合规范;红外感应传感器用于监测暂存间门的开关状态,防止医疗废物非法丢弃或泄漏。当监测参数出现异常时,系统立即触发预警,通知环保管理部门及时处置;同时,系统自动记录监测数据,形成环保管理档案,为环保检查与追溯提供数据支撑。某医院通过该体系实现监控后,污水处理达标率提升至 100%,医疗废物暂存环境违规事件发生率降至 0。

三、物联网环境监控的智能预警与联动调控机制

(一) 多级智能预警机制构建

物联网环境监控系统构建了多级智能预警机制,根据环境参数异常程度与影响范围,划分一般预警、重要预警、紧急预警三个等级,实现精准预警与高效处置。一般预警针对参数轻微偏离阈值、影响范围较小的情况(如公共区域温湿度轻微波动),系统通过平台弹窗提醒管理人员关注;重要预警针对参数明显偏离阈值、可能影响诊疗安全或环境质量的情况(如药房温度接近阈值上限),系统通过短信、APP 推送等方式通知管理人员及时处置;紧急预警针对参数严重偏离阈值、存在重大安全风险的情况(如手术室洁净度严重超标、污水处理参数异常),系统立即触发声光报警,同步通知相关科室负责人、医院管理层,并启动应急处置流程。

同时,系统支持预警信息的追溯与分析,自动记录预警发生时间、原因、处置过程与结果,为优化环境管理策略提供数据支撑。多级智能预警机制的构建,确保了环境异常能够被及时发现、精准处置,有效降低了环境风险。

(二) 设备智能联动调控机制实现

物联网环境监控系统实现了与环境调控设备的智能联动,构建了“监测-分析-预警-调控”的闭环管理机制,提升环境管理的自动化水平。通过打通环境管理

平台与空调、新风系统、空气净化设备、净化系统、冷链设备等调控设备的控制接口，实现设备的远程控制与智能调控。当监测到环境参数超出阈值时，系统无需人工干预，自动向相关调控设备下发控制指令，调整设备运行参数，直至环境参数恢复正常。

例如，当手术室温度高于 25℃ 时，系统自动下发指令提升空调制冷功率；当公共区域 PM2.5 浓度超标时，系统自动启动空气净化设备并提升运行档位；当冷藏药房温度高于 8℃ 时，系统自动启动制冷设备并检查设备运行状态。智能联动调控机制的实现，大幅减少了人工干预，提升了环境调控的及时性与精准性，同时降低了管理人员的工作负荷。

四、物联网环境监控的应用价值与成效

（一）保障诊疗安全，降低感染风险

物联网环境监控系统通过对手术室、ICU、新生儿科等核心区域环境参数的精准监控与智能调控，确保了诊疗环境的合规性，有效降低了医院感染风险。例如，手术室洁净度的精准控制，减少了手术过程中细菌、病毒等有害微生物的污染，降低了手术感染率；新生儿科温湿度的精细化调控，为新生儿提供了安全的生长环境，减少了感染并发症的发生。某医院应用该系统后，全院医院感染发生率降低 30%，核心诊疗区域感染发生率降低 50%，有效保障了患者诊疗安全。

（二）提升就医体验，优化服务质量

通过对门诊、住院楼等公共区域环境质量的优化，物联网环境监控系统有效提升了患者就医体验。公共区域 PM2.5 浓度的降低、CO₂ 浓度的稳定、噪声的控制，为患者营造了清新、舒适、安静的就医环境；药房与试剂库房环境的精准监控，保障了药品与试剂质量，提升了患者用药安全与诊疗效果。某医院应用该系统后，患者就医环境满意度提升 35%，整体服务质量评分提升 15%，增强了患者对医院的信任度。

（三）降低管理成本，提升运营效率

物联网环境监控系统的自动化、智能化特性，大幅降低了医院环境管理的人工成本与运营成本。智能联动调控机制减少了人工干预，管理人员工作量减少 60%；根据环境参数与人员流量动态调整调控设备运行参数，实现了精准能耗控制，某医院应用该系统后，环境调控设备能耗降低 25%；药品与试剂变质损耗率

的降低，减少了资源浪费，降低了医院运营成本。同时，系统自动生成环境管理档案，为医院质量控制、环保检查提供了精准数据支撑，提升了管理效率。

（四）助力合规管理，提升管理水平

物联网环境监控系统的应用，助力医院实现了环境管理的合规化与标准化。系统对环境参数的全程监测与记录，形成了可追溯的环境管理档案，满足了《医院感染管理办法》《医疗机构水污染物排放标准》等相关法律法规的要求，为环保检查、质量评估提供了可靠的数据依据。同时，通过对环境数据的深度分析，能够发现环境管理过程中的薄弱环节，为优化环境管理策略提供数据支撑，推动医院环境管理从“经验管理”向“精准管理”转型，提升了医院整体管理水平。

第四章 云计算与云原生技术在医院信息化管理中的应用研究

第一节 云计算服务模式与医疗信息化架构适配

一、主流云计算服务模式解析

（一）基础设施即服务（IaaS）：底层资源弹性支撑

基础设施即服务（IaaS）作为云计算最基础的服务模式，通过虚拟化技术将服务器、存储设备、网络资源等底层硬件资源池化，以按需租用的方式为医院提供弹性计算与存储支撑。该模式下，医院无需投入大量资金购置物理硬件，可根据信息化建设需求灵活申请计算节点、存储空间、带宽资源，实现资源的动态扩容与缩容。例如，在医院开展大型医疗数据筛查、基因测序等高密度计算任务时，可通过 IaaS 快速扩容计算资源，任务完成后释放资源，降低资源闲置成本。

IaaS 服务具备高可用性与容错性优势，通过多可用区部署、数据冗余备份等技术，保障医院核心业务系统的稳定运行，避免因单点故障导致的服务中断。目前，医院应用 IaaS 的主要形式包括私有云 IaaS 部署（依托医院自有数据中心构建）、公有云 IaaS 租用（接入阿里云、腾讯云等公有云厂商资源）以及混合云 IaaS 架构（融合私有云与公有云资源，实现核心业务私有部署、非核心业务公有托管）。IaaS 为医疗信息化架构提供了灵活、高效的底层资源支撑，是医院实现信息化降本增效的重要基础。

（二）平台即服务（PaaS）：中间件与开发环境赋能

平台即服务（PaaS）在 IaaS 底层资源之上，提供了涵盖数据库服务、中间件、开发工具、运行环境等在内的一站式开发与部署平台，聚焦于为医院信息化应用开发提供技术赋能。该模式下，医院信息技术人员无需关注底层硬件资源与基础软件的运维，可直接基于 PaaS 平台提供的标准化组件与开发工具，快速构建、部署与迭代医疗信息化应用，如门诊预约系统、住院管理系统、医疗数据分析系统等。

PaaS 平台具备较强的可扩展性与兼容性,支持多种开发语言与框架,能够适配医院不同类型的应用开发需求;同时,集成了数据备份、安全防护、负载均衡等通用功能,降低了应用开发与运维的复杂度。例如,PaaS 平台提供的分布式数据库服务,可满足医院电子病历、健康档案等海量医疗数据的存储与高效查询需求;大数据分析组件则支持对医疗数据的挖掘与分析,为临床诊疗与医院管理提供决策支撑。PaaS 的应用,大幅提升了医院信息化应用的开发效率,加速了医疗信息化创新场景的落地。

(三) 软件即服务 (SaaS): 轻量化应用快速部署

软件即服务 (SaaS) 以订阅制模式为医院提供成熟的轻量化信息化应用,医院无需进行应用开发与底层环境部署,通过互联网即可直接使用软件功能,是最易落地的云计算服务模式。该模式下,软件厂商负责应用的开发、升级、运维与安全防护,医院只需根据实际需求支付订阅费用,大幅降低了信息化建设的初期投入与技术门槛。

在医疗领域,SaaS 应用主要覆盖非核心业务场景,如医院 OA 系统、采购管理系统、患者随访系统等。例如,患者随访 SaaS 平台可实现患者出院后的自动化随访提醒、随访数据采集与分析,无需医院单独开发系统;疫情防控登记 SaaS 系统可快速部署于医院入口,实现患者信息登记、体温监测数据统计等功能。SaaS 应用具备快速部署、易用性强、维护成本低的优势,能够满足医院碎片化、轻量化的信息化需求,与 IaaS、PaaS 形成互补,丰富了医院云计算应用的场景覆盖。

(四) 云原生服务: 容器化与微服务架构升级

云原生服务是基于云计算架构演进的新一代服务模式,以容器化、微服务、DevOps 等技术为核心,实现应用的快速迭代、弹性伸缩与高可用部署。容器化技术(如 Docker)将应用及其依赖环境打包为标准化容器,确保应用在不同环境下的一致性运行;微服务架构则将大型应用拆分为多个独立的微服务模块,每个模块可单独开发、部署与升级,提升了应用的灵活性与可维护性;DevOps 技术实现了开发与运维的协同联动,加速了应用迭代效率。

云原生服务相比传统云计算服务,更适配医疗信息化系统的高并发、高可用、高安全需求,能够有效解决传统单体医疗系统升级困难、扩展受限、运维复杂等问题。例如,基于云原生架构构建的电子病历系统,可将病历采集、存储、查询、分析等功能拆分为独立微服务,支持按需扩容某一模块资源,提升系统应对高峰

访问的能力；同时，容器化部署使得系统升级无需整体停机，保障了业务的连续性。云原生服务正成为医院信息化架构升级的核心方向，推动医疗信息化从“传统云部署”向“原生云架构”转型。

二、医疗信息化架构核心需求与痛点

（一）核心需求：高可用、高安全、可扩展、数据协同

医疗信息化架构的核心需求围绕临床诊疗与医院管理的安全性、高效性展开，具体体现为四个维度：一是高可用性，医疗核心业务系统（如 HIS、EMR、PACS）需 7×24 小时连续运行，任何服务中断都可能影响诊疗安全，因此架构需具备极强的容错与故障恢复能力；二是高安全性，医疗数据包含患者隐私信息与核心诊疗数据，敏感度极高，架构需构建全链路安全防护体系，防范数据泄露、篡改与非法访问；三是可扩展性，随着医院规模扩大、业务场景丰富（如远程医疗、AI 辅助诊断），信息化系统需能够快速扩容资源，适配业务增长需求；四是数据协同，医院内部各系统（HIS、EMR、PACS）之间、院区间以及医院与区域医疗平台之间需实现数据互通共享，支撑连续诊疗与协同管理。

（二）传统架构痛点：资源利用率低、扩展受限、运维复杂

传统医疗信息化架构多采用“物理服务器+单体应用”的部署模式，存在诸多痛点：一是资源利用率低，为保障业务高峰运行，医院需按照峰值需求配置物理服务器，大部分时间资源处于闲置状态，造成硬件投入浪费；二是扩展能力受限，单体应用的架构设计导致系统扩容需整体升级硬件，无法实现按需弹性扩展，难以应对突发业务高峰（如突发公共卫生事件期间的诊疗需求激增）；三是运维复杂度高，传统架构依赖大量人工进行硬件维护、系统升级与故障排查，运维成本高且效率低，同时系统升级需整体停机，影响业务连续性；四是数据协同困难，各系统采用独立的数据库与部署环境，形成“数据孤岛”，跨系统、跨院区数据共享需进行复杂的接口开发，协同效率低下。

三、云计算服务模式与医疗信息化架构的适配策略

（一）混合云架构：核心业务私有部署，非核心业务公有托管

混合云架构融合了私有云与公有云的优势，是当前医院信息化架构的主流适配方案。针对医疗核心业务（如 EMR、HIS、PACS、核心数据存储），采用私

有云 IaaS/PaaS 部署,依托医院自有数据中心构建独立的云计算环境,实现对核心数据与业务的绝对掌控,保障数据安全与服务可控;针对非核心业务(如患者随访、OA 办公、在线预约、医疗数据分析),采用公有云 SaaS/IaaS 服务,借助公有云厂商的资源优势,实现快速部署与弹性扩展,降低信息化建设成本。^①

混合云架构通过专用网络通道实现私有云与公有云的互联互通,确保数据在安全可控的前提下实现协同共享。例如,医院可将核心电子病历数据存储于私有云,同时将非核心的随访数据同步至公有云 SaaS 平台,实现随访业务的轻量化运营;在开展大型医疗数据挖掘时,可将私有云中的脱敏数据同步至公有云大数据平台,利用公有云的海量计算资源完成分析任务。某三甲医院采用混合云架构后,核心业务可用性提升至 99.99%,信息化建设成本降低 35%,资源利用率提升 60%。

(二) 云原生架构:微服务拆分与容器化部署适配核心业务

针对核心医疗业务系统的升级需求,采用云原生架构进行适配改造,通过微服务拆分与容器化部署,解决传统单体系统的扩展与运维痛点。将传统单体 EMR、HIS 系统拆分为多个独立的微服务模块(如病历采集模块、处方管理模块、住院登记模块、收费模块等),每个模块基于容器化技术部署,实现独立的资源分配、升级与运维。例如,当门诊挂号量激增时,可单独对挂号微服务模块进行资源扩容,不影响其他模块的运行;系统升级时,可针对单个微服务模块进行灰度发布,避免整体停机。

云原生架构集成了服务网格、动态服务发现、自动伸缩等组件,进一步提升了系统的高可用性与可扩展性。服务网格实现了微服务之间的智能通信与流量管理,动态服务发现确保了容器实例的灵活调度,自动伸缩组件可根据业务负载自动调整容器数量,实现资源的精准匹配。某医院基于云原生架构改造 EMR 系统后,系统响应速度提升 40%,升级停机时间缩短至 0,运维人员工作量减少 50%,有效支撑了临床诊疗业务的高效开展。

(三) 分层 SaaS 适配:轻量化应用覆盖碎片化需求

针对医院碎片化、轻量化的信息化需求,采用分层 SaaS 适配策略,通过不同类型的 SaaS 应用覆盖全业务场景。在行政办公领域,部署 OA、采购管理、

① 周靖云,蒋清,任健.云计算在医院信息化管理中的作用及影响[J].现代医院,2023,23(03):422-424.

人力资源管理 SaaS 系统，提升行政效率；在患者服务领域，部署在线预约、报告查询、患者教育等 SaaS 应用，改善患者就医体验；在科研教学领域，部署科研数据管理、在线培训等 SaaS 平台，支撑科研与教学工作；在公共卫生领域，部署疫情防控、传染病上报等 SaaS 系统，提升应急处置能力。

分层 SaaS 适配的核心是实现 SaaS 应用与医院核心系统的对接，通过标准化接口将 SaaS 应用数据同步至医院私有云数据中心，避免形成新的“数据孤岛”。例如，在线预约 SaaS 系统将患者预约数据同步至 HIS 系统，实现预约与挂号的无缝衔接；患者随访 SaaS 平台将随访数据同步至 EMR 系统，丰富患者诊疗档案。分层 SaaS 应用的部署，无需医院投入大量资源进行系统开发与维护，能够快速满足多样化的信息化需求，与混合云、云原生架构形成互补，构建全方位的医疗信息化服务体系。

第二节 电子病历与健康档案的云原生存储及跨院区共享平台构建

一、电子病历与健康档案的云原生存储体系构建

（一）云原生存储核心技术选型

电子病历与健康档案的云原生存储体系需满足海量数据存储、高并发访问、高可靠性、数据安全可控等核心需求，核心技术选型聚焦于分布式存储、容器化存储管理、数据加密与备份三大方向。在分布式存储技术方面，采用分布式文件存储（如 Ceph、GlusterFS、TStor、DASTor）与分布式数据库（如 TiDB、OceanBase、GoldenDB、TDSQL、GaussDB、Tendis）协同架构：分布式文件存储用于存储电子病历中的文档、影像、音频等非结构化数据，具备高扩展性与高容错性，支持 PB 级数据存储；分布式数据库用于存储患者基本信息、诊疗记录等结构化数据，支持高并发读写与数据分片存储，提升数据查询与处理效率。

在容器化存储管理方面，采用容器存储接口（CSI）实现存储资源与容器化应用的无缝对接，通过存储类（StorageClass）动态为电子病历、健康档案相关微服务分配存储资源，实现存储资源的弹性伸缩与按需分配。在数据加密与备份方面，采用全生命周期加密策略，数据在存储、传输、使用过程中均进行加密处理（存储加

密采用 AES-256 算法，传输加密采用 SSL/TLS 协议）；同时，构建“本地备份 + 异地容灾”的双重备份体系，通过定时快照、增量备份等技术，确保数据在极端情况下的可恢复性。某医院构建的云原生存储体系，支持日均 10 万份电子病历的新增存储，数据查询响应时间缩短至 50ms 以内，数据可靠性提升至 99.999%。

（二）存储架构设计：分层存储与冷热数据分离

为提升存储效率、降低存储成本，电子病历与健康档案云原生存储体系采用“分层存储 + 冷热数据分离”的架构设计。分层存储将存储资源划分为高性能存储层、标准存储层与归档存储层：高性能存储层采用 SSD 磁盘构建，用于存储高频访问的核心数据（如当前住院患者电子病历、近期诊疗记录），保障高并发访问场景下的响应速度；标准存储层采用 SAS 磁盘构建，用于存储中频访问数据（如近 3-5 年的门诊病历、健康档案），平衡存储性能与成本；归档存储层采用大容量机械磁盘或对象存储构建，用于存储低频访问的归档数据（如 5 年以上的历史病历、健康档案），大幅降低长期存储成本。

冷热数据分离通过智能数据迁移策略实现，系统根据数据访问频率自动识别热数据（高频访问）与冷数据（低频访问），并将热数据迁移至高性能存储层，冷数据迁移至标准存储层或归档存储层；同时，支持冷数据的压缩存储与 deduplication（重复数据删除）处理，进一步提升存储利用率。例如，某医院通过冷热数据分离策略，将 90% 的历史归档数据迁移至归档存储层，存储成本降低 40%，同时核心热数据查询效率提升 35%。

（三）存储安全与合规保障

电子病历与健康档案包含大量患者隐私数据，存储体系需严格遵循《电子病历应用规范》《个人信息保护法》《数据安全法》等法律法规，构建全链路安全与合规保障机制。在访问控制方面，采用基于角色的访问控制（RBAC）与最小权限原则，为医护人员、管理人员、科研人员等不同角色分配差异化的存储访问权限，同时记录详细的访问日志，实现访问行为的全程追溯；对于敏感数据（如艾滋病、性病等特殊疾病诊疗记录），采用额外的权限审批机制，确保数据访问的合规性。

在数据防护方面，除全生命周期加密外，部署数据防泄漏（DLP）系统，防范数据非法拷贝、传输与外泄；构建存储安全审计系统，对数据的存储、访问、修改、删除等操作进行实时监控与审计，及时发现并处置安全风险。在合规性验

证方面，定期对存储体系进行安全测评与合规检查，确保数据存储符合相关法律法规要求；同时，保留完整的存储日志与备份记录，为数据追溯与合规检查提供可靠依据。通过全方位的安全与合规保障机制，确保电子病历与健康档案数据的安全可控。

二、跨院区共享平台的云原生架构设计与实现

（一）平台架构设计：微服务化与云原生部署

跨院区电子病历与健康档案共享平台采用云原生微服务架构设计，整体分为基础设施层、平台服务层、应用服务层与安全保障层四个层级。基础设施层基于混合云 IaaS 资源构建，为平台提供弹性计算、存储与网络支撑；平台服务层包含微服务注册发现、配置中心、API 网关、消息队列、分布式事务等核心组件，支撑微服务的协同运行；应用服务层拆分为数据采集与同步、数据标准化处理、数据共享与交换、权限管理、统计分析等微服务模块，实现跨院区共享的核心功能；安全保障层贯穿各层级，提供身份认证、数据加密、访问控制、安全审计等全方位安全服务。

平台采用容器化部署模式，所有微服务模块均打包为容器镜像，通过 Kubernetes 进行编排与管理，实现服务的自动伸缩、故障自愈与滚动升级。例如，当多院区同时发起大量数据查询请求时，Kubernetes 自动扩容数据共享微服务的容器实例，提升平台并发处理能力；当某一容器实例出现故障时，系统自动重启或替换实例，保障服务连续性。云原生架构的采用，使平台具备极强的扩展性与可用性，能够适配多院区、大规模数据共享需求。

（二）核心功能实现：数据同步、标准化与共享交互

数据同步功能：采用实时增量同步与定时全量同步相结合的方式，实现各院区电子病历与健康档案数据向共享平台的汇聚。通过部署数据同步微服务，监听各院区 EMR 系统的数据库变更日志（如 MySQL 的 binlog），实时捕获新增、修改的病历数据，经加密处理后同步至平台分布式存储系统；同时，每日凌晨执行全量同步任务，校验数据完整性，确保各院区数据与平台数据一致。针对大型影像数据（如腰椎核磁、脂肪抑制成像等），采用断点续传与压缩传输技术，提升同步效率。

数据标准化处理：构建医疗数据标准化引擎，对各院区同步至平台的异构数

据（不同厂商 EMR 系统产生的非标准化数据）进行清洗、转换与标准化处理。通过映射字典（如疾病编码、药品编码、手术编码映射至国家标准编码），统一数据格式与编码规范；采用自然语言处理（NLP）技术，提取非结构化病历文本中的关键信息（如诊断结果、用药信息、检查结论），转化为结构化数据，提升数据的可复用性。

数据共享与交互功能：平台提供标准化 API 接口与 Web 门户，支持各院区医护人员通过权限认证后查询共享数据。例如，医生在诊疗时可通过平台快速查询患者在其他院区的历史病历、检查报告、用药记录等信息，支撑连续诊疗；同时，平台支持跨院区诊疗数据的实时写入，实现“一次诊疗、多院共享”。此外，平台提供数据统计分析功能，为医院管理层提供多院区医疗服务质量、资源利用效率等决策支撑数据。

（三）多院区协同机制：权限协同与冲突解决

权限协同机制：构建统一的跨院区权限管理体系，实现各院区用户权限的集中管理与协同联动。平台采用统一身份认证（SSO）技术，各院区用户通过统一账号密码登录平台，系统根据用户所属院区、角色自动分配共享数据访问权限；支持权限的分级授权，院区间可通过权限申请与审批流程，临时或长期开放特定数据的访问权限。例如，当 A 院区医生需要查阅 B 院区患者的特殊诊疗记录时，可通过平台提交权限申请，经 B 院区相关负责人审批通过后获取访问权限。

冲突解决机制：针对多院区同时修改同一患者病历数据可能产生的冲突，平台采用“时间戳优先 + 人工仲裁”的冲突解决策略。系统记录每条数据的最后修改时间戳与修改院区，当检测到冲突时，自动保留最新修改的数据，并标记冲突状态；同时，通知相关院区医护人员进行人工核对与仲裁，确保数据的准确性。此外，平台保留数据修改的完整版本记录，支持数据回溯，为冲突解决与责任追溯提供依据。

三、应用价值与成效

（一）提升诊疗效率与质量，改善患者体验

云原生存储体系实现了电子病历与健康档案的高效存储与快速查询，跨院区共享平台打破了“数据孤岛”，使医护人员能够快速获取患者全生命周期诊疗数据，避免重复检查与误诊误治，提升诊疗效率与质量。例如，某医疗集团通过跨

院区共享平台,实现了5家院区电子病历的实时共享,医生诊疗时查询患者历史病历的时间从平均15分钟缩短至1分钟以内,重复检查率降低35%,误诊率降低20%;患者在多院区间转诊时无需重复携带病历资料,转诊流程简化,就医等待时间缩短40%,就医体验大幅提升。

（二）优化资源配置,降低运营成本

云原生存储的分层存储与冷热数据分离策略,大幅降低了电子病历与健康档案的长期存储成本;跨院区共享平台实现了医疗数据与资源的集中管理,避免了各院区重复建设信息化系统,降低了整体信息化投入。某医疗集团通过构建云原生存储与跨院区共享平台,信息化建设总成本降低30%,存储成本降低45%;同时,集中化的数据分析与管理,优化了医疗资源配置,使优质医疗资源能够在多院区间高效流转,提升了资源利用效率。^①

（三）支撑科研创新与公共卫生决策

云原生存储体系汇聚了多院区海量电子病历与健康档案数据,为医学科研提供了丰富的数据资源;跨院区共享平台的标准化数据处理功能,提升了数据的可用性,支持科研人员开展多中心、大样本的医学研究。例如,某医疗集团基于共享平台的标准化数据,开展了心血管疾病发病规律与危险因素研究,研究周期缩短50%,研究成果的准确性与可靠性大幅提升。同时,平台能够快速汇总多院区医疗数据,为区域公共卫生决策(如传染病防控、慢性病管理)提供实时、精准的数据支撑,提升公共卫生服务能力。

（四）强化数据安全与合规管理

云原生存储与跨院区共享平台构建的全链路安全防护体系,有效保障了电子病历与健康档案数据的安全与合规。通过数据加密、访问控制、安全审计等技术,防范了数据泄露、篡改与非法访问风险;统一的权限管理与合规检查机制,确保了数据使用符合相关法律法规要求。某医院应用该体系后,未发生一起数据安全事件,通过了国家医疗数据安全专项检查,数据合规管理水平显著提升,增强了患者对医院的数据信任度。

^① 张杨. 云计算技术在医院后勤信息化建设中的应用研究[J]. 长江信息通信, 2022, 35 (10): 127-129.

第三节 云计算支撑的医疗大数据挖掘与临床决策分析应用

一、医疗大数据的核心特征与云计算适配性

（一）医疗大数据核心特征：多源异构、海量高维、实时性强

医疗大数据源于临床诊疗、公共卫生、科研实验等多个场景，呈现出鲜明的多源异构、海量高维、实时性强等核心特征。从数据来源看，涵盖电子病历、影像数据（CT、MRI、超声）、检验化验数据、基因测序数据、wearable 设备监测数据、医院运营数据等多种类型；从数据形态看，包含结构化数据（如患者基本信息、诊疗编码）、半结构化数据（如病历文书）、非结构化数据（如影像、音频），异构性显著。

从数据规模与维度看，单家三甲医院年均产生的医疗数据量可达 PB 级，且每条数据包含多个维度的关联信息（如患者诊疗数据关联人口学、遗传学、环境因素等），呈现海量高维特性；从实时性需求看，临床诊疗场景中患者体征监测、急诊救治等数据需实时处理与分析，为诊疗决策提供即时支撑，对数据处理的时效性要求极高。这些特征决定了医疗大数据挖掘需依托具备强大算力、海量存储与高效数据处理能力的技术架构，而云计算恰好为其提供了适配的技术支撑。

（二）云计算与医疗大数据挖掘的适配性优势

云计算的弹性算力、分布式存储与高效数据处理能力，与医疗大数据挖掘的技术需求高度适配，形成三大核心优势。一是弹性算力支撑海量数据并行处理，医疗大数据挖掘涉及复杂的算法模型训练（如深度学习、机器学习）与大规模数据运算，云计算通过 IaaS 层的弹性扩容能力，可根据挖掘任务需求快速调度海量计算节点，实现数据的并行处理与模型的快速迭代，大幅提升挖掘效率。例如，基因测序数据的分析任务需处理海量碱基序列数据，依托云计算的弹性算力可将分析周期从数天缩短至数小时。

二是分布式存储适配多源异构数据管理，云计算 PaaS 层提供的分布式数据库、对象存储等服务，可实现对医疗多源异构数据的统一存储与管理，通过数据分片、副本备份等技术，保障数据存储的安全性与可用性，同时支持结构化、非结构化数据的高效检索，为大数据挖掘提供便捷的数据访问支撑。三是云原生大数据平台简化挖掘流程，主流云计算厂商提供的大数据分析平台（如阿里云 E-MapReduce、腾讯云 TDSQL），集成了数据清洗、转换、建模、分析等全流

程工具，医院无需从零构建大数据挖掘架构，可直接基于平台开展挖掘工作，降低技术门槛与运维成本。

二、云计算支撑的医疗大数据挖掘关键技术与流程

（一）关键技术：分布式计算、机器学习、自然语言处理

分布式计算技术是云计算支撑医疗大数据挖掘的核心基础，主要包括 Hadoop、Spark 等框架。Hadoop 基于分布式文件系统（HDFS）实现海量数据的分布式存储，通过 MapReduce 编程模型实现数据的并行计算，适用于离线大规模数据处理；Spark 则在 Hadoop 基础上优化了计算引擎，支持内存计算，大幅提升了数据处理速度，适用于实时性要求较高的大数据挖掘场景（如临床实时监测数据挖掘）。两者协同应用，可满足医疗大数据离线挖掘与实时分析的多样化需求。

机器学习技术是医疗大数据价值转化的核心工具，涵盖分类、回归、聚类、深度学习等多种算法。分类算法（如逻辑回归、随机森林）可用于疾病风险预测、病理类型识别等场景；回归算法可用于医疗费用预测、疾病进展趋势分析；聚类算法可用于患者群体分层、疾病亚型划分；深度学习算法（如卷积神经网络 CNN、循环神经网络 RNN）则在医学影像识别、病历文本分析等领域具备显著优势。自然语言处理（NLP）技术可实现对非结构化病历文本的结构化处理，提取其中的关键诊疗信息（如诊断结果、用药记录、症状描述），转化为可用于挖掘分析的结构化数据，提升医疗大数据的利用率。

（二）核心流程：数据采集与预处理、模型构建与训练、结果验证与应用

数据采集与预处理：基于云计算平台构建多源医疗数据采集体系，通过标准化接口对接医院 HIS、EMR、PACS 等系统，以及 wearable 设备、区域医疗平台等外部数据来源，实现数据的集中汇聚；借助云计算 PaaS 层的数据清洗工具，对采集的数据进行去噪、去重、缺失值填充、异常值处理等预处理操作；通过数据标准化技术（如统一疾病编码、药品编码），解决多源数据的异构性问题，形成高质量的挖掘数据集。

模型构建与训练：基于云计算的弹性算力平台，根据挖掘目标选择适配的算法模型（如疾病预测选择深度学习模型、患者分层选择聚类模型），利用预处理

后的数据集开展模型训练；通过云计算平台的分布式训练能力，实现大规模数据集的快速模型迭代，同时利用平台的超参数调优工具，优化模型性能。模型构建过程中，可依托云计算平台的可视化工具，实时监控模型训练效果，提升模型构建效率。

结果验证与应用：通过预留的测试数据集对训练完成的模型进行性能验证，评估模型的准确率、召回率、F1 值等指标，确保模型的可靠性；将验证通过的模型部署至云计算平台，通过 API 接口对接临床诊疗系统、医院管理系统等应用场景，实现挖掘结果的落地应用；同时，建立模型迭代优化机制，基于新产生的医疗数据持续优化模型，提升模型的适应性与准确性。

三、临床决策分析核心应用场景

（一）疾病风险预测与早期筛查

基于云计算的医疗大数据挖掘技术，可构建疾病风险预测模型，实现对慢性病、恶性肿瘤等疾病的早期筛查与风险预警，为临床早干预、早治疗提供支撑。通过采集患者的人口学数据、既往病史、体检数据、基因数据、生活习惯数据等多维度信息，利用机器学习算法（如随机森林、深度学习）构建风险预测模型，预测患者未来一定时期内患某种疾病的风险概率。

例如，某医院基于云计算平台构建的高血压风险预测模型，整合了辖区内 10 万余名居民的健康数据，模型准确率达 85% 以上，可提前 6-12 个月预测高血压发病风险；通过将模型部署至社区健康管理系统，为社区医生提供居民高血压风险评估工具，针对高风险人群开展个性化干预（如饮食指导、运动建议、定期监测），使辖区高血压发病率降低 22%。此外，在肺癌、乳腺癌等恶性肿瘤早期筛查中，通过融合影像数据与临床数据构建深度学习模型，可实现对早期病灶的精准识别，筛查准确率提升 30% 以上，大幅提高了肿瘤的早期检出率。

（二）精准诊疗方案推荐

依托云计算平台的海量医疗数据挖掘能力，可构建精准诊疗方案推荐模型，为临床医生提供个性化的诊疗建议，提升诊疗的精准性与有效性。通过挖掘历史诊疗数据中相似病例的诊疗方案与疗效信息，结合患者的具体病情（如疾病类型、分期、并发症、基因特征），利用协同过滤、深度学习等算法，为当前患者推荐最优诊疗方案（如用药方案、手术方案、康复计划）。

例如，某三甲医院基于云计算平台构建的肿瘤精准诊疗推荐系统，整合了 5 万余例肿瘤患者的历史诊疗数据，通过挖掘不同治疗方案与患者基因特征、病情分期的匹配关系，为新入院肿瘤患者推荐个性化治疗方案。应用该系统后，医生制定诊疗方案的时间从平均 2 小时缩短至 30 分钟，治疗有效率提升 18%，患者住院周期缩短 25%。同时，系统可实时整合最新的医学指南与科研成果，持续优化诊疗方案推荐，确保方案的科学性与前沿性。

（三）临床风险预警与并发症防控

基于云计算的实时大数据分析能力，可构建临床风险预警模型，实现对住院患者术后并发症、重症患者病情恶化等风险的实时预警，提升临床风险防控能力。通过实时采集患者的体征监测数据、检验化验数据、治疗数据等，利用流式计算技术（如 Spark Streaming）对数据进行实时分析，结合预设的风险预警模型，当检测到风险信号时立即向医护人员发出预警。

例如，某医院在 ICU 部署的重症患者病情恶化预警系统，基于云计算平台实时分析患者的心电、血氧、血压等 10 余项体征数据，当数据出现异常波动时，系统可提前 1-2 小时发出预警，预警准确率达 88%。应用该系统后，ICU 患者病情恶化的早期干预率提升 45%，死亡率降低 15%。在术后并发症防控中，通过挖掘术后患者的体温、血常规、伤口愈合等数据，构建并发症预警模型，可提前预警感染、出血等并发症风险，使术后并发症发生率降低 30% 以上。

（四）合理用药与药物不良反应预测

通过云计算挖掘医疗大数据中的用药数据、患者不良反应数据、基因数据等，可构建合理用药推荐模型与药物不良反应预测模型，提升临床用药安全性与合理性。合理用药推荐模型基于患者的疾病诊断、肝肾功能、过敏史、合并用药情况等，推荐适配的药物、剂量与用药频次，避免药物滥用与不合理联用；药物不良反应预测模型则通过分析患者基因特征与药物的相互作用，预测患者使用某种药物后发生不良反应的风险，为个体化用药提供支撑。

例如，某医院构建的合理用药预警系统，依托云计算平台挖掘了 10 万余例用药案例数据，当医生开具处方时，系统实时分析处方合理性，对不合理用药（如药物过敏风险、剂量过高、药物相互作用禁忌）发出预警，预警准确率达 92%。应用该系统后，医院不合理用药率降低 40%，药物不良反应发生率降低 28%，极大提升了临床用药安全。

第四节 元原生技术在智慧医疗场景应用效果评估

一、评估体系构建原则与核心维度

（一）评估体系构建原则

云原生技术在智慧医疗场景的应用效果评估体系，需遵循针对性、全面性、可量化、动态性四大核心原则。针对性原则：聚焦智慧医疗核心场景（如电子病历系统、远程医疗平台、智能监护系统），结合云原生技术的核心优势（如弹性伸缩、高可用、快速迭代）设定评估指标，确保评估结果贴合临床与管理实际需求。全面性原则：覆盖技术性能、业务效能、经济效益、安全合规等多个维度，全面评估云原生技术应用的综合价值，避免单一维度评估导致的片面性。

可量化原则：尽量采用量化指标开展评估，避免模糊的定性描述，确保评估结果客观、可比，便于不同场景、不同医院之间的效果对比。动态性原则：智慧医疗场景与云原生技术均处于持续发展阶段，评估体系需具备动态调整能力，根据技术迭代、业务拓展及时优化评估指标与权重，确保评估体系的适应性与时效性。

（二）核心评估维度

技术性能维度：聚焦云原生技术支撑智慧医疗系统运行的核心技术指标，包括系统可用性、响应速度、并发处理能力、弹性伸缩效率、运维效率等，评估云原生技术对系统技术性能的提升效果。业务效能维度：评估云原生技术对临床诊疗、医院管理等业务场景的赋能效果，包括诊疗效率、诊疗质量、患者体验、管理效率等核心指标，体现技术应用的业务价值。

经济效益维度：评估云原生技术应用带来的成本节约与效益提升，包括信息化建设成本、运维成本、医疗资源浪费减少、诊疗效率提升带来的经济效益等指标，量化技术应用的经济价值。安全合规维度：评估云原生技术应用对智慧医疗系统安全与合规性的保障效果，包括数据安全防护能力、系统故障恢复能力、合规性符合程度等指标，确保技术应用的安全性与合规性。

二、典型智慧医疗场景应用效果评估

（一）云原生电子病历系统应用效果评估

技术性能评估：系统基于云原生架构，实现了微服务化和容器化部署，具备

高弹性与高可用性。在性能指标上,依托分布式存储与分布式数据库协同,支持数千并发用户的高频读写,核心业务操作响应时延控制在毫秒级。通过存储计算分离与多副本一致性协议,确保了医疗数据的强一致性与零丢失,系统可用性达到 99.99% 以上。同时,具备自动故障转移与横向扩展能力,可灵活应对业务高峰期的资源需求。

业务效能评估:云原生架构打破了传统医疗信息孤岛,实现了病历数据的全院级实时共享与互联互通。医生站调阅病历平均耗时缩短,影像资料加载流畅,显著提升了诊疗效率与临床决策质量。支持多租户模式,满足集团化医院多院区一体化管理需求。通过电子病历评级与互联互通成熟度测评,助力医院通过国家等级评审。此外,DevOps 敏捷开发模式支持业务需求快速迭代,平均版本发布周期缩短。^①

经济效益评估:通过硬件资源池化与容器混合部署,物理服务器利用率提升,有效降低了初期硬件采购成本。基于弹性伸缩能力,按需使用资源,避免了传统架构的过度投资。运维层面,自动化运维工具减少人工干预,降低了运维人力成本。长期来看,标准化数据接口降低了第三方系统对接成本,并通过对临床数据的深度利用,为科研与精细化管理提供支撑,挖掘了数据资产的潜在价值。

(二) 云原生远程医疗平台应用效果评估

技术性能评估:云原生远程医疗平台基于微服务架构构建,支持多院区、多终端的协同接入,系统并发接入能力提升 4 倍,可同时支撑 500+ 远程会诊场景运行;视频传输延迟控制在 150ms 以内,画面清晰度与稳定性显著提升,解决了传统远程医疗平台的卡顿、延迟问题;平台可用性达 99.99%,确保远程诊疗业务的连续运行;通过容器化部署,平台升级无需停机,新功能上线时间从数周缩短至数天,迭代效率提升 70%。

业务效能评估:远程会诊效率提升 60%,从患者申请会诊到会诊完成的平均时间从 3 天缩短至 1.2 天,偏远地区患者无需长途奔波即可获得优质医疗资源;远程影像诊断效率提升 55%,基层医院影像报告审核时间从 24 小时缩短至 6 小时以内,提升了基层诊疗质量;远程培训覆盖范围扩大 3 倍,每年可为基层医护人员提供 1000+ 场远程培训,基层医护人员诊疗水平显著提升。

^① 陈昊,陈伟,刘利,等.医疗质量管理云平台的研发与应用[J].中国数字医学,2016,11(11):80-82+113.

经济效益评估：远程医疗平台减少了患者跨区域就医的交通、住宿成本，每年为患者节约费用数千万元；优质医疗资源下沉减少了基层医院的转诊率，基层医院诊疗收入提升 25%；平台集中化部署避免了各院区重复建设，信息化建设成本降低 45%。安全合规评估：平台采用统一身份认证、数据加密传输等安全技术，确保远程诊疗数据的安全可控；平台运行符合《远程医疗服务管理规范》等要求，通过了医疗数据安全专项检查。

（三）云原生智能监护系统应用效果评估

技术性能评估：云原生智能监护系统采用边缘计算 + 云端协同架构，边缘节点实现体征数据的实时采集与本地分析，云端实现数据汇总与模型训练，数据传输延迟控制在 100ms 以内，确保预警的实时性；系统支持多类型监护设备的接入，兼容性提升 80%；云端弹性算力支撑模型快速迭代，模型优化周期从 1 个月缩短至 1 周；系统可用性达 99.99%，故障自愈时间缩短至 5 分钟以内，保障了监护业务的连续运行。

业务效能评估：重症患者体征异常发现时间缩短至 30 秒以内，应急处置响应效率提升 50%，重症患者救治成功率提升 12%；术后患者康复监护效率提升 40%，医护人员术后巡查工作量减少 50%，术后并发症发生率降低 35%；特殊患者定位精度提升至 1-3 米，患者走失率降至 0，跌倒事件发生率降低 65%，患者安全保障能力显著提升。

经济效益评估：智能监护系统减少了医护人员的人工监护工作量，可使每名护士负责的患者数量提升 30%，降低了人力成本；术后并发症发生率降低减少了医疗费用支出，每年为医院节约医疗成本数百万元；患者救治成功率提升与就医体验改善，提升了医院的品牌影响力，间接带来了经济效益增长。安全合规评估：系统具备完善的数据加密与访问控制机制，患者隐私数据安全得到有效保障；监护数据记录完整，可实现全程追溯，符合医疗质量控制与合规要求。

三、评估结果应用与优化建议

（一）评估结果应用方向

优化技术架构：基于评估结果，针对云原生技术应用中存在的性能瓶颈（如特定场景下的响应延迟、并发处理不足），优化微服务拆分、容器编排策略，提升系统技术性能；针对兼容性、扩展性不足等问题，完善技术标准与接口规范，

提升系统的适配能力。

指导业务落地：根据不同智慧医疗场景的应用效果评估结果，明确云原生技术的核心赋能场景，优先在效果显著的场景（如电子病历系统、智能监护系统）加大推广力度；针对效果不佳的场景，分析原因并优化业务流程与技术方案，提升技术与业务的适配性。

支撑决策规划：评估结果为医院信息化建设决策提供数据支撑，帮助医院合理规划云原生技术应用的优先级与资源投入；为区域医疗信息化建设提供参考，推动云原生技术在区域智慧医疗体系中的规模化应用。

（二）云原生技术在智慧医疗应用的优化建议

加强技术适配性优化：针对智慧医疗场景的特殊性（如实时性要求高、数据敏感性强），优化云原生技术方案，提升技术与业务的适配性；加强边缘计算与云原生技术的融合应用，降低数据传输延迟，提升实时处理能力。

构建人才培养体系：云原生技术在智慧医疗的应用需要具备医疗业务知识与云原生技术能力的复合型人才，医院应加强与高校、企业的合作，构建人才培养与引进体系，提升内部技术团队的专业能力。

完善安全合规体系：持续优化云原生环境下的安全防护方案，加强容器安全、微服务安全、数据安全防护技术的应用；建立动态合规检查机制，确保技术应用符合不断更新的法律法规要求。

推动技术标准统一：联合行业协会、医疗机构、技术厂商制定云原生技术在智慧医疗应用的技术标准与规范，统一接口标准、数据格式、安全要求等，提升不同系统、不同医院之间的互操作性，推动云原生技术在智慧医疗领域的规模化、规范化应用。

第五章 人工智能与新一代通信技术 融合应用研究

第一节 AI 与通信技术（5G/ 边缘计算）融合的 医疗技术基础与架构

一、核心技术基础：AI、5G、边缘计算的技术特性与融合逻辑

（一）三大核心技术的医疗适配特性

人工智能（AI）技术为医疗场景提供核心智能决策能力，其机器学习、深度学习、计算机视觉等分支在医疗领域呈现精准适配特性。例如，深度学习算法可通过海量医学影像数据训练实现病灶精准识别，计算机视觉技术能辅助分析病理切片、内镜影像等微观图像，自然语言处理技术可解析非结构化电子病历提取关键诊疗信息，为临床决策提供数据支撑。AI 技术的核心优势在于对高维、异构医疗数据的深度挖掘与价值转化，解决传统医疗中经验依赖、诊断偏差等问题。

5G 作为新一代通信技术，其超高带宽（eMBB）、超低时延（uRLLC）、海量连接（mMTC）三大核心特性精准匹配医疗场景需求。超高带宽可支撑 4K/8K 高清医学影像、远程手术实时视频流的稳定传输，单用户下行速率可达 10Gbps，解决传统网络影像传输卡顿、延迟问题；超低时延（端到端时延低至 1ms）为远程精准手术、实时生命体征监测等时延敏感场景提供保障；海量连接能力可实现医院内多终端设备（如智能监护仪、可穿戴设备、物联网传感器）的同时接入，支撑智慧病房、全流程诊疗监测等规模化应用。

边缘计算技术通过将计算资源下沉至靠近数据产生端的边缘节点，弥补了云端计算的时延短板。在医疗场景中，边缘节点可就近处理实时性要求高的医疗数据（如生命体征监测数据、术中影像数据），减少数据向云端传输的距离与时延，同时降低核心网络带宽占用；此外，边缘计算具备本地数据存储与处理能力，可在网络中断等极端情况下保障关键医疗业务的连续运行，提升医疗系统的可靠性与数据安全性。

（二）技术融合逻辑：协同互补构建智能医疗支撑体系

AI 与 5G、边缘计算的融合并非简单叠加，而是形成“通信赋能数据传输、边缘支撑实时处理、AI 提供智能决策”的协同互补逻辑，构建全链条智能医疗支撑体系。从数据流转维度看，5G 网络负责将医疗终端采集的多源数据（影像、体征、病历等）高效、实时传输至边缘节点或云端；边缘计算承担实时性数据的预处理与即时分析，为本地医疗场景提供快速响应；AI 算法则在边缘或云端开展深度模型训练与复杂决策分析，形成精准诊断结果或诊疗建议。

从技术短板互补维度看，5G 解决了 AI 模型部署中的数据传输瓶颈，使 AI 算法能快速获取海量分布式医疗数据进行训练与迭代；边缘计算弥补了云端 AI 处理的时延缺陷，使 AI 模型能在时延敏感医疗场景（如远程手术、紧急救治）中即时生效；AI 技术则提升了 5G 与边缘计算的资源利用效率，通过智能调度算法优化网络带宽、计算资源的分配，实现资源按需动态适配医疗业务需求。三者融合形成“数据-传输-处理-决策”的闭环，为智慧医疗场景提供全栈式技术支撑。

二、融合架构设计：分层架构与核心组件

（一）总体分层架构：从终端到云端的全链路设计

AI 与 5G/边缘计算融合的医疗架构采用分层设计理念，从上至下分为应用层、AI 智能层、边缘计算层、5G 传输层、终端感知层五个核心层级，各层级协同联动实现全链路智能医疗服务。该架构通过层级化分工，确保数据传输的高效性、计算处理的实时性、智能决策的精准性，同时具备良好的扩展性与兼容性，可适配不同医疗场景的个性化需求。

终端感知层作为数据采集源头，涵盖医学影像设备（CT、MRI、超声仪）、生命体征监测设备（心电监护仪、血氧仪）、可穿戴健康设备、手术机器人、内镜设备等各类医疗终端，负责采集诊疗过程中的影像、体征、操作等多源数据；5G 传输层承担数据传输核心职责，通过 5G 基站、核心网构建高速、低时延、高可靠的传输网络，实现终端数据向边缘节点或云端的实时传输；边缘计算层部署在医院本地或区域边缘节点，提供就近计算、存储与预处理能力，支撑实时性医疗业务的快速响应；AI 智能层集成各类 AI 算法模型与智能决策引擎，负责数据的深度分析与智能决策，输出诊断结果、诊疗建议等核心信息；应用层则面向具体医疗场景，提供远程手术、智能诊断、实时监护、应急救援等差异化医疗服务。

（二）核心组件与功能实现

5G 医疗专用网络组件：采用网络切片技术构建医疗专用切片，实现医疗业务与公网业务的隔离，保障医疗数据传输的安全性与带宽专属化。通过核心网功能虚拟化（NFV）与网络功能编排（MANO）技术，实现医疗切片资源的动态调度，根据不同医疗业务（如远程手术、影像传输）的带宽、时延需求，灵活分配网络资源。同时，部署 5G 边缘网关设备，实现终端设备与 5G 网络的无缝对接，支持多种医疗设备接口的标准化适配。

边缘计算节点组件：每个边缘节点集成计算服务器、存储设备、AI 加速芯片（GPU、FPGA）等硬件资源，以及容器化部署平台、数据预处理引擎、本地 AI 模型库等软件组件。边缘节点可实现医疗数据的本地缓存与预处理（去噪、去重、格式转换），减少无效数据传输；部署轻量级 AI 模型（如实时体征异常检测模型、术中影像快速分析模型），实现实时性数据的即时分析与响应；通过边缘云管理平台，实现多边缘节点的协同调度与资源统一管理，提升边缘计算资源的利用率。

AI 智能引擎组件：包含模型训练平台、模型推理引擎、数据标注工具三大核心模块。模型训练平台依托云端或边缘节点的算力资源，支持基于海量医疗数据的 AI 模型训练与迭代优化，兼容深度学习、机器学习等多种算法框架；模型推理引擎负责将训练完成的 AI 模型部署至边缘或云端，实现对输入医疗数据的快速推理与分析，输出精准的诊断结果或决策建议；数据标注工具支持医护人员对医疗数据进行人工标注与修正，为 AI 模型训练提供高质量标注数据集，提升模型精度。

安全防护组件：贯穿全架构各层级，构建全方位安全防护体系。终端层采用设备身份认证、数据采集加密技术，确保源头数据安全；传输层通过 5G 加密传输、虚拟专用网络（VPN）等技术，保障数据传输过程不被窃取或篡改；边缘与云端采用访问控制、权限管理、入侵检测等技术，防范非法访问与攻击；同时，部署医疗数据脱敏引擎，对患者隐私数据进行脱敏处理，符合《个人信息保护法》《医疗数据安全指南》等合规要求。

三、架构适配的关键医疗场景需求

（一）实时性诊疗场景适配需求

实时性诊疗场景（如远程精准手术、紧急救治、实时生命体征监测）对架构的时延与可靠性要求极高，融合架构通过“5G 超低时延传输 + 边缘计算本地处理”的协同设计精准适配。在远程手术场景中，5G 网络实现手术机器人操作指令与高清手术视频的 1ms 级低时延传输，边缘节点就近处理手术影像的实时分析数据，AI 模型即时识别手术区域的关键组织与风险点，为术者提供实时操作指导；在紧急救治场景中，边缘节点实时处理患者的生命体征数据，AI 模型快速判断病情危急程度并给出初步救治建议，同时通过 5G 网络将患者数据同步至云端专家系统，实现多学科专家的实时会诊支持。^①

（二）海量数据处理场景适配需求

海量数据处理场景（如医学影像批量分析、大规模体检数据筛查、基因组数据分析）对架构的算力与数据传输能力要求突出，融合架构通过“5G 超高带宽传输 + 边缘 - 云端协同计算”的模式适配。5G 网络的超高带宽特性支撑 PB 级医学影像数据的快速传输，避免传统网络传输效率低的问题；边缘节点负责数据的预处理与初步筛选，剔除无效数据并完成格式标准化；云端则依托强大的算力资源部署复杂 AI 模型，开展海量数据的深度分析与模型训练，实现大规模数据的高效处理与价值挖掘。例如，在大规模肺癌筛查场景中，5G 网络将基层医院的 CT 影像快速传输至边缘节点，边缘 AI 模型完成初步病灶筛查，再将疑似病例数据传输至云端进行精准诊断，大幅提升筛查效率与覆盖面。

第二节 智能诊断辅助与通信系统集成

一、智能诊断辅助系统的核心构成与技术支持

（一）核心功能模块构成

智能诊断辅助系统围绕临床诊断全流程构建核心功能模块，主要包括数据采集与预处理模块、多模态数据融合分析模块、精准诊断推理模块、结果展示与交

① 张羽翔. 5G 环境下远程医疗急救视频传输的计算机网络实时性能分析与优化改进 [J]. 软件, 2025, 46 (10): 141-143.

互模块。数据采集与预处理模块通过标准化接口对接各类医疗设备，采集影像、体征、病历等多源数据，并完成数据清洗、去噪、标准化处理，形成高质量诊断数据集；多模态数据融合分析模块采用深度学习融合算法，将不同类型的医疗数据（如影像数据与临床病历数据）进行融合分析，挖掘数据间的关联关系，提升诊断的全面性与准确性；精准诊断推理模块集成针对不同疾病的专用 AI 模型（如肿瘤影像诊断模型、心血管疾病诊断模型），通过模型推理输出疾病诊断结果、病灶定位、病情分期等核心信息；结果展示与交互模块以可视化方式向医护人员呈现诊断结果，支持医护人员对诊断结果进行修正与反馈，形成人机协同诊断闭环。

（二）AI 与通信技术的核心支撑作用

AI 技术为智能诊断辅助系统提供核心智能能力，通过深度学习、计算机视觉等算法实现对医疗数据的精准分析与诊断推理。例如，基于卷积神经网络（CNN）的医学影像诊断模型，可通过海量标注影像数据训练，实现对肺部结节、乳腺钙化点等微小病灶的精准识别，识别准确率可达 95% 以上；基于自然语言处理（NLP）的病历分析模型，可从非结构化病历文本中提取患者的症状、病史、用药史等关键信息，为诊断推理提供全面数据支撑。同时，AI 模型的持续迭代优化能力，可通过不断学习新的医疗数据与临床经验，提升诊断系统的适应性与准确性。

5G 与边缘计算技术为智能诊断辅助系统提供高效数据传输与实时处理支撑。5G 网络实现多源医疗数据的高速、实时传输，解决了传统网络中影像数据传输慢、多终端数据同步难的问题；边缘计算技术使 AI 诊断模型能够就近部署与运行，实现对实时性要求高的诊断任务（如术中影像诊断、急诊影像分析）的快速响应，减少诊断时延。此外，5G 的海量连接能力支持医院内多台诊断设备与智能诊断系统的同时接入，实现诊断资源的规模化共享与高效利用。

二、智能诊断辅助与通信系统的集成架构与关键技术

（一）集成架构设计：全链路协同一体化

智能诊断辅助与通信系统采用“终端 - 通信 - 计算 - 智能”全链路协同的集成架构，实现诊断数据的无缝流转与诊断服务的高效协同。架构底层为医疗终端层，涵盖各类影像设备、监测设备等，通过 5G 模组或边缘网关接入 5G 通信

网络；中间层为通信与计算层，由 5G 传输网络与边缘计算节点组成，负责数据的实时传输、本地预处理与初步 AI 推理；上层为智能诊断应用层，集成智能诊断辅助系统的核心功能模块，通过 API 接口与医院现有信息系统（HIS、EMR、PACS）对接，实现诊断结果的全流程应用。

该集成架构具备三大核心特性：一是数据传输一体化，通过 5G 网络实现医疗终端数据向智能诊断系统的直接传输，无需经过多环节转接，减少数据丢失与时延；二是计算资源协同化，边缘节点与云端协同为智能诊断提供算力支撑，实时性诊断任务由边缘节点处理，大规模数据训练与复杂诊断任务由云端承担，提升资源利用效率；三是应用对接标准化，通过 HL7 FHIR、DICOM 等医疗数据标准，实现智能诊断系统与医院现有信息系统的无缝对接，确保诊断结果能够直接融入临床诊疗流程，提升诊断服务的实用性。

（二）关键集成技术

医疗数据标准化集成技术：采用 DICOM 标准实现医学影像数据的标准化封装与传输，确保不同厂商影像设备产生的数据能够被智能诊断系统兼容识别；通过 HL7 FHIR 标准实现临床数据（病历、体征、用药信息）的标准化交互，解决不同系统间的数据格式差异问题。同时，部署数据格式转换引擎，实现非标准医疗数据向标准格式的自动转换，提升数据集成的兼容性与效率。

边缘 - 云端 AI 模型协同部署技术：采用模型拆分部署策略，将 AI 诊断模型的轻量级推理部分部署在边缘节点，负责实时性数据的快速推理；将模型训练与复杂推理部分部署在云端，负责模型的持续训练与优化，并将优化后的模型参数同步至边缘节点。通过模型参数增量同步技术，减少模型更新时的数据传输量，提升模型迭代效率。同时，采用模型选择调度算法，根据诊断任务的复杂度与实时性需求，自动选择边缘或云端模型进行处理，确保诊断效率与准确性的平衡。

5G 网络切片与 QoS 保障技术：为智能诊断业务专属划分 5G 网络切片，通过网络功能编排技术为切片分配专属带宽与计算资源，确保诊断数据传输的优先级；采用 QoS（服务质量）保障机制，对诊断数据传输的时延、带宽、丢包率等指标进行实时监控与动态调整，当网络质量下降时，自动触发资源调度策略，保障诊断数据传输的稳定性与可靠性。例如，在远程影像诊断场景中，通过 QoS 保障技术将影像传输的丢包率控制在 0.01% 以内，确保诊断影像的清晰度与完整性。

安全可信集成技术：构建“端-边-云”全链路安全集成体系，终端层采用设备身份认证与数据采集加密技术，防止设备伪造与数据泄露；传输层采用 5G 加密传输与 VPN 技术，保障数据传输过程的安全可控；边缘与云端采用访问控制、权限管理、数据脱敏等技术，防范非法访问与数据滥用。同时，部署区块链存证模块，对诊断数据的采集、传输、分析、应用全流程进行存证，实现诊断数据的可追溯与不可篡改，提升诊断结果的可信度与法律有效性。

三、集成应用场景与实践效果

（一）远程影像智能诊断集成应用

在远程影像智能诊断场景中，智能诊断辅助系统与 5G 通信系统深度集成，实现基层医院影像数据向上级医院智能诊断中心的快速传输与精准诊断。基层医院通过 5G 网络将患者 CT、MRI 等影像数据传输至边缘节点，边缘 AI 模型完成初步病灶筛查与数据预处理，再将疑似病例影像与初步分析结果传输至云端智能诊断系统；云端系统通过多模态数据融合分析，结合患者临床病历数据给出精准诊断结果与治疗建议，诊断结果通过 5G 网络实时反馈至基层医院，同时同步至患者电子病历系统。

某区域医疗联合体的实践数据显示，该集成应用使基层医院影像诊断时间从平均 24 小时缩短至 30 分钟以内，疑难病例诊断准确率提升 35%，基层医院转诊率降低 28%。5G 网络的超高带宽确保了高清影像的快速传输，边缘计算的本地处理能力减少了数据传输时延，AI 诊断模型则提升了诊断的精准性与效率，有效解决了基层医院影像诊断能力不足的问题。

（二）术中实时智能诊断与导航集成应用

在复杂手术场景中，智能诊断辅助系统与 5G+ 边缘计算系统集成，实现术中实时影像分析与手术导航。手术过程中，内镜、手术显微镜等设备采集的实时影像通过 5G 网络传输至边缘节点，边缘 AI 模型实时分析影像中的手术区域、关键组织、病灶边界等信息，输出手术导航指令；导航指令通过 5G 网络低时延传输至手术机器人或术者操作终端，为术者提供精准的操作指引，避免损伤正常组织。同时，边缘节点将术中影像与诊断数据实时同步至云端专家系统，专家可通过系统实时监控手术过程，必要时给出远程指导建议。

某三甲医院在神经外科手术中的应用实践表明，该集成应用使手术精准度提

升 40%，手术时间缩短 25%，术后并发症发生率降低 32%。5G 的超低时延传输保障了导航指令的即时响应，边缘计算的本地处理能力确保了术中影像分析的实时性，AI 诊断模型则为手术提供了精准的影像解读与导航支撑，大幅提升了复杂手术的安全性与有效性。

（三）急诊多模态智能诊断集成应用

在急诊场景中，智能诊断辅助系统与 5G 通信系统集成，实现多源急诊数据的实时采集、融合分析与快速诊断。急诊患者的生命体征数据（心电、血氧、血压）通过 5G 可穿戴设备实时传输至边缘节点，急诊影像数据（超声、CT）通过 5G 网络快速传输至智能诊断系统，AI 模型融合分析体征数据与影像数据，快速判断患者病情危急程度，给出初步诊断结果与急救建议；同时，系统通过 5G 网络将患者数据同步至急诊信息系统与多学科会诊平台，实现急诊医生与专科医生的实时协同，提升急诊救治效率。

某医院急诊科室的应用实践显示，该集成应用使急诊患者平均确诊时间从 45 分钟缩短至 10 分钟以内，危重患者救治成功率提升 18%，多学科会诊响应时间缩短 60%。5G 的实时传输能力确保了急诊数据的快速汇聚，AI 模型的多模态融合分析能力提升了急诊诊断的效率与准确性，通信系统与诊断系统的集成则实现了急诊救治的全流程协同，为患者争取了宝贵的救治时间。

四、集成应用的挑战与优化方向

（一）核心挑战

技术层面，不同医疗设备接口标准不统一，导致智能诊断系统与终端设备的集成难度较大；5G 网络在医院复杂环境（如地下机房、厚重墙体）中的信号覆盖稳定性有待提升；边缘计算节点的算力资源有限，难以支撑多并发、复杂 AI 模型的实时推理。数据层面，医疗数据隐私性强，跨机构、跨区域数据共享存在合规风险；不同医院的医疗数据格式差异大，数据质量参差不齐，影响 AI 模型的诊断准确性。应用层面，医护人员对智能诊断系统的接受度与操作熟练度不足，人机协同诊断的流程有待优化；智能诊断结果的法律认可度不足，限制了系统在临床诊断中的深度应用。

（二）优化方向

技术优化方面，推动医疗设备接口标准化建设，制定智能诊断与通信系统集

成的技术规范；优化 5G 网络在医院复杂环境中的覆盖方案，采用小基站、信号增强器等设备提升信号稳定性；提升边缘计算节点的算力配置，采用算力虚拟化、动态调度技术提升资源利用效率。数据优化方面，构建医疗数据安全共享平台，采用联邦学习、差分隐私等技术实现数据“可用不可见”，兼顾数据共享与隐私保护；建立医疗数据质量管控体系，通过数据清洗、标注审核等技术提升数据质量，为 AI 模型提供可靠数据支撑。

应用优化方面，加强医护人员的系统操作培训，优化人机协同诊断流程，提升系统的易用性；推动智能诊断结果的临床验证与法律认证，建立诊断结果责任划分机制；开展多中心临床应用试点，积累应用经验并持续优化系统性能，推动智能诊断辅助与通信系统集成应用的规模化落地。

第三节 基于人工智能 + 通信融合的医疗资源智能分配与调度

一、核心技术支持与融合逻辑

（一）关键技术选型与适配特性

人工智能技术为医疗资源分配调度提供核心决策能力，主要采用强化学习、遗传算法、深度学习等算法模型。强化学习通过与医疗服务环境的实时交互，持续优化资源分配策略，适配动态变化的诊疗需求；遗传算法擅长解决多目标优化问题，可在床位、医护人员、设备等多类资源间实现全局最优分配；深度学习模型则通过挖掘历史诊疗数据、资源使用数据，精准预测区域医疗需求峰值与资源缺口。这些算法的核心优势在于能够处理医疗场景中多维度、动态化的复杂约束条件，突破传统经验式调度的局限性。

新一代通信技术（5G/ 边缘计算）为智能分配调度提供高效数据传输与实时处理支撑。5G 的超高带宽特性可实现全区域医疗数据（就诊量、床位占用率、设备运行状态等）的高速汇聚，单用户下行速率 10Gbps 的传输能力确保海量实时数据无延迟同步；超低时延（端到端 1ms 级）特性保障调度指令的即时下达与执行反馈，适配急诊资源调度、突发公共卫生事件应急响应等时延敏感场景；海量连接能力可实现医院内、区域间多终端设备（医护终端、床位监测设备、移动诊疗设备）的同时接入，支撑规模化资源调度协同。边缘计算通过本地节点就

近处理实时调度数据，减少向云端传输的时延，提升调度决策的实时性，同时保障网络中断时核心调度功能的连续运行。

（二）技术融合逻辑：数据－传输－决策－执行闭环

人工智能与通信技术的融合形成“全链路协同”的医疗资源调度支撑体系，构建“数据采集－实时传输－智能决策－指令执行－反馈优化”的闭环流程。从数据流转维度，分布在医院各科室、区域医疗节点的终端设备采集就诊量、床位状态、医护人员工作量、设备利用率等多源数据，通过 5G 网络实时传输至边缘节点或云端调度平台；边缘节点对实时数据进行预处理（清洗、去重、格式标准化），并运行轻量级 AI 模型完成初步调度分析；云端平台部署复杂 AI 优化模型，结合历史数据与实时数据开展全局资源分配决策，生成最优调度方案；调度指令通过 5G 网络即时下达至各医疗终端，同时将执行结果反馈至调度平台，驱动 AI 模型持续迭代优化。

从功能互补维度，5G 解决了传统调度中数据传输滞后、多终端协同不畅的问题，为 AI 模型提供实时、全面的数据支撑；边缘计算弥补了云端决策的时延缺陷，确保紧急场景下调度指令的即时响应；AI 技术则提升了资源调度的精准性与全局优化能力，通过数据挖掘与预测分析，实现医疗资源从“被动响应”向“主动预判”的转变。三者融合使医疗资源调度具备实时性、精准性、全局性三大核心特性，有效提升资源利用效率。

二、医疗资源智能分配与调度的核心场景实践

（一）院内核心医疗资源动态分配

针对院内床位、医护人员、诊疗设备等核心资源，构建基于 AI+5G 的动态分配系统，实现资源与诊疗需求的精准匹配。在床位分配场景中，系统通过 5G 网络实时采集各科室床位占用率、患者病情严重程度、预计住院时长等数据，AI 模型结合历史住院数据预测各科室床位需求，采用强化学习算法动态调整床位资源，优先保障危重患者床位需求，同时优化床位周转效率。例如，某三甲医院部署的智能床位调度系统，通过 5G 网络实时同步全院 2000 余张床位状态，AI 模型精准预测各科室床位缺口，实现跨科室床位动态调剂，使危重患者床位等待时间从平均 2 小时缩短至 30 分钟以内，全院床位周转率提升 25%。

在医护人员调度场景中，系统实时采集医护人员工作量、专业资质、在岗

状态等数据，结合各科室就诊量、急诊患者数量等实时需求，通过遗传算法优化医护人员排班与调配方案。当某科室出现就诊高峰或突发紧急情况时，系统通过 5G 网络即时向备用医护人员推送调度指令，同时同步患者病情信息与诊疗需求，实现医护资源的快速响应。应用该系统后，医院医护人员工作负荷均衡度提升 40%，急诊患者医护响应时间缩短 50%。在诊疗设备调度场景中，通过 5G 网络实现 CT、MRI、超声仪等大型设备运行状态的实时监测，AI 模型预测设备使用需求，动态分配设备检查时段，避免设备闲置或患者等待时间过长，设备利用率提升 35%，患者检查等待时间缩短 40%。

（二）区域医疗资源协同调度

基于 AI+5G 构建区域医疗资源协同调度平台，打破不同医院、不同层级医疗机构间的资源壁垒，实现区域内医疗资源的优化配置与高效共享。平台通过 5G 网络整合区域内三甲医院、社区医院、乡镇卫生院等各类医疗机构的资源数据（专家资源、设备资源、床位资源）与诊疗需求数据（就诊量、疑难病例分布、突发公共卫生事件），AI 模型采用全局优化算法，根据患者病情严重程度、地理位置、医疗机构服务能力等因素，制定最优资源调配方案。

在分级诊疗场景中，平台通过 AI 模型对患者病情进行智能分级，引导轻症患者在社区医院就诊，疑难重症患者精准转诊至三甲医院，同时通过 5G 网络实现患者电子病历、检查影像等数据的实时共享，避免重复检查。某区域医疗联合体的实践显示，该协同调度平台使区域内分级诊疗率提升 30%，基层医院就诊率提升 28%，三甲医院疑难重症接诊效率提升 45%。在突发公共卫生事件应急调度场景中，平台通过 5G 网络实时汇聚疫情数据、医疗资源储备数据，AI 模型快速预测医疗资源需求峰值，动态调配区域内的医护人员、防护物资、诊疗设备，实现资源的精准投放。在某次疫情防控中，该平台实现区域内医护人员跨机构调配响应时间缩短至 2 小时以内，防护物资调配效率提升 60%，有效保障了疫情防控的医疗资源供给。

（三）应急医疗资源快速调度

针对突发疾病救治、交通事故救援等应急场景，构建基于 AI+5G+ 边缘计算的应急医疗资源快速调度系统，实现“院前 - 院中 - 院后”全流程资源协同。系统通过 5G 网络实时连接急救车、现场救援终端、医院急诊中心，边缘节点就近处理实时救援数据，AI 模型快速制定救援资源调配方案与救治路径。在院前急

救阶段，急救车通过 5G 网络将患者生命体征数据、现场影像数据实时传输至边缘节点，AI 模型快速评估患者病情严重程度，提前调度医院急诊资源（如急诊医生、手术间、急救设备），同时规划最优转运路线，避开交通拥堵。

例如，某城市部署的应急医疗调度系统，当发生交通事故时，系统通过 5G 网络在 30 秒内完成患者病情评估，1 分钟内调度就近急救车与医院急诊资源，同时通过 AI 模型优化转运路线，使患者平均到院时间缩短 20%，危重患者救治成功率提升 18%。在院中急救阶段，系统通过 5G 网络实现急诊各科室资源的协同调度，AI 模型根据患者病情动态调配医护人员、诊疗设备，确保急救流程高效衔接。院后康复阶段，系统结合患者康复情况，通过 5G 网络调度社区康复资源，实现患者从医院到社区的无缝康复衔接，提升康复效果。

三、调度系统的核心架构与关键技术实现

（一）总体架构设计

医疗资源智能分配与调度系统采用“终端感知层-5G 传输层-边缘计算层-AI 调度层-应用层”五层架构，各层级协同实现资源调度的全流程智能化。终端感知层部署在各级医疗机构、急救车、社区卫生服务中心等节点，涵盖床位监测设备、医护人员定位终端、诊疗设备传感器、患者体征监测设备等，负责采集各类资源数据与诊疗需求数据；5G 传输层通过 5G 基站、核心网构建高速、低时延、高可靠的传输网络，实现多源数据的实时传输与调度指令的即时下达；边缘计算层部署在区域医疗中心或医院本地，提供数据预处理、实时调度分析、本地决策能力，保障紧急场景下的即时响应；AI 调度层集成模型训练平台、调度决策引擎、数据挖掘引擎等核心组件，负责资源需求预测、调度方案优化与决策生成；应用层面向院内调度、区域协同、应急救援等不同场景，提供个性化的调度服务与可视化管理界面。

（二）关键技术实现

多源数据融合与标准化技术：采用 HL7 FHIR、DICOM 等医疗数据标准，实现不同医疗机构、不同类型终端设备数据的标准化交互；部署数据融合引擎，通过深度学习算法对结构化数据（床位状态、就诊量）与非结构化数据（病历文本、影像数据）进行融合分析，提升数据的完整性与可用性。同时，采用数据脱

敏技术对患者隐私数据进行处理,符合医疗数据安全合规要求。^①

AI 调度模型优化与部署技术:采用模型轻量化技术,将复杂的全局优化模型拆分部署在边缘节点与云端,边缘节点运行轻量级模型处理实时调度需求,云端运行复杂模型开展全局资源优化与模型训练;通过模型增量更新技术,将云端优化后的模型参数实时同步至边缘节点,提升模型迭代效率。同时,采用模型自适应调整机制,根据医疗服务环境的动态变化(如突发就诊高峰、资源供给变化),自动调整模型参数,确保调度方案的适应性。

5G 网络切片与 QoS 保障技术:为医疗资源调度业务专属划分 5G 网络切片,实现调度数据与其他业务数据的隔离传输,保障调度数据的传输优先级;采用 QoS 保障机制,对调度数据传输的时延、带宽、丢包率等指标进行实时监控与动态调整,当网络质量下降时,自动触发资源调度策略,确保调度指令的即时下达与数据的稳定传输。例如,在应急救援场景中,通过网络切片技术将调度数据传输的时延控制在 1ms 以内,丢包率控制在 0.01% 以下。

可视化调度与协同管理技术:构建可视化调度管理平台,通过图表、地图等形式实时展示医疗资源分布、诊疗需求分布、调度方案执行进度等信息,支持医护人员、管理人员直观掌握资源调度状态;部署多终端协同管理模块,实现医院内、区域内不同终端设备的协同联动,确保调度指令在各节点的高效执行。

四、应用挑战与优化方向

(一) 核心挑战

技术层面,不同医疗机构的信息系统标准不统一,导致数据共享与集成难度较大;AI 调度模型的泛化能力不足,在不同医疗场景、不同区域的适配性有待提升;5G 网络在偏远地区、地下空间等复杂环境的信号覆盖稳定性不足,影响调度数据的实时传输。管理层面,跨机构、跨区域的医疗资源调度涉及多方利益协调,协同机制不完善;医护人员对智能调度系统的接受度与操作熟练度不足,影响系统的落地效果。数据层面,医疗数据隐私性强,跨机构数据共享存在合规风险;部分医疗机构的数据质量参差不齐,影响 AI 模型的调度精度。

^① 樊怡. 人工智能在公立医院档案管理信息化中的应用探索 [J]. 临床医药实践, 2025, 34 (07): 558-560.

（二）优化方向

技术优化方面，推动区域医疗信息系统标准化建设，制定统一的数据接口与通信协议；加强 AI 调度模型的迁移学习与自适应训练，提升模型在不同场景的适配性；优化 5G 网络覆盖方案，采用小基站、信号增强器等设备提升复杂环境的信号稳定性。管理优化方面，建立跨机构、跨区域的医疗资源调度协同机制，明确各方职责与利益分配；加强医护人员与管理系统的系统操作培训，优化系统交互界面，提升系统的易用性。数据优化方面，构建医疗数据安全共享平台，采用联邦学习、差分隐私等技术实现数据“可用不可见”；建立数据质量管控体系，通过数据清洗、标注审核等技术提升数据质量，为 AI 模型提供可靠支撑。

第四节 智能医患交互与通信体验场景优化

一、核心技术支持与融合价值

（一）关键技术选型与交互适配

人工智能技术为智能医患交互提供核心智能能力，主要采用自然语言处理（NLP）、语音识别、计算机视觉、推荐算法等技术。NLP 技术实现医患对话的智能理解与精准响应，支持医疗术语的精准识别、语义分析与意图判断；语音识别技术实现医患语音交互的实时转写与精准识别，识别准确率可达 98% 以上，适配不同口音、不同语速的语音输入；计算机视觉技术支持人脸识别、手势交互等多模态交互方式，提升交互的便捷性；推荐算法根据患者病情、诊疗历史，精准推送个性化健康宣教内容、诊疗建议等信息。

新一代通信技术（5G/ 边缘计算）为医患交互提供高效、稳定的通信支撑，优化交互体验。5G 的超高带宽特性支撑 4K/8K 高清视频交互、医学影像实时共享，解决传统视频交互卡顿、画质模糊的问题；超低时延特性保障医患语音、视频交互的实时性，端到端时延低至 1ms 级，实现“面对面”般的交互体验；海量连接能力支持多终端设备（患者手机、病房交互平板、医护移动终端）的同时接入，支撑多场景医患交互协同。边缘计算通过本地节点就近处理交互数据，减少数据传输时延，提升交互响应速度；同时，边缘节点具备本地数据存储能力，在网络中断时保障核心交互功能的连续运行，提升交互的可靠性。

（二）技术融合价值：重构医患交互模式

人工智能与通信技术的融合打破了传统医患交互的时空限制，重构“全流程、多场景、个性化”的医患交互模式，实现三大核心价值。一是提升交互效率，通过智能语音、视频交互等方式，减少患者排队等待时间，简化诊疗流程；二是优化交互体验，实现个性化、精准化的医患交互服务，提升患者的就医满意度；三是拓展交互场景，从传统的院内面对面交互，延伸至远程问诊、居家康复指导、健康管理等多场景，提升医疗服务的连续性与普惠性。例如，通过 AI+5G 构建的远程医患交互系统，患者无需到院即可与专家进行高清视频问诊，实现“足不出户看专家”，大幅降低患者的就医成本与时间成本。

二、智能医患交互的核心场景与体验优化实践

（一）远程精准问诊与多模态交互

构建基于 AI+5G 的远程精准问诊系统，实现医患之间的高清视频交互、多模态数据共享与智能辅助诊断，优化远程问诊体验。系统通过 5G 网络支撑 4K 高清视频交互，结合 AI 降噪算法消除环境噪音，提升语音交互清晰度；患者可通过手机、平板等终端上传医学影像、检查报告等数据，5G 网络实现数据的快速传输，AI 模型实时对数据进行初步分析，为医生问诊提供辅助支撑；医生通过系统实时查看患者数据，结合视频观察患者症状，给出精准诊断建议。同时，系统支持语音转文字功能，自动生成问诊记录，减少医生文书工作量。

某三甲医院的远程问诊系统实践显示，该系统使专家响应患者问诊的时间从平均 24 小时缩短至 2 小时以内，患者平均问诊时间缩短 35%，问诊满意度提升 40%。针对偏远地区患者，系统通过 5G 网络覆盖解决了传统远程问诊网络卡顿的问题，实现优质医疗资源的下沉，偏远地区患者远程问诊覆盖率提升至 85%。此外，系统支持多学科专家协同问诊，通过 5G 网络实现多专家同时接入视频问诊，为疑难病例患者提供综合诊疗建议，提升远程问诊的精准性。

（二）智慧病房医患交互体验优化

在病房场景中，基于 AI+5G 构建智慧病房交互系统，整合病房交互平板、智能摄像头、全向麦克风等终端设备，实现患者与医护人员、家属之间的多场景智能交互，优化住院体验。患者通过病房交互平板可实现一键呼叫医护人员、查看诊疗计划、预约检查、获取个性化健康宣教内容等功能；通过 AI 语音助手，

患者可语音查询病情、用药信息，系统通过 NLP 技术精准理解患者需求并给出响应。医护人员通过移动终端实时接收患者呼叫，查看患者需求，远程解答患者疑问，减少往返病房的次数，提升工作效率。

家属探视场景中，系统支持预约式远程视频探视，家属通过手机小程序预约探视时段，系统通过人脸识别+手机号验证完成身份核验；探视时，通过 5G 网络实现高清视频交互，结合 AI 隐私遮挡技术，自动模糊患者床号、病历等敏感信息，保障患者隐私。某医院的智慧病房实践显示，该系统使患者呼叫医护人员的响应时间从平均 5 分钟缩短至 1 分钟以内，医护人员查房效率提升 30%，家属远程探视覆盖率提升至 90%，患者住院满意度提升 45%。此外，系统可与病房内的智能输液泵、生命体征监测仪等设备联动，当患者生命体征异常或输液完成时，自动触发视频呼叫，及时通知医护人员处理。

（三）居家康复与健康管理交互

基于 AI+5G 构建居家康复与健康管理交互系统，实现患者出院后与医护人员的持续交互，提升康复效果与健康管理效率。系统通过 5G 可穿戴设备实时采集患者的生命体征数据（心率、血压、血氧）、康复训练数据（运动轨迹、动作规范度），数据通过 5G 网络实时传输至边缘节点或云端平台；AI 模型对数据进行实时分析，判断患者康复进度，识别康复训练中的不规范动作，通过语音、视频等方式即时给出纠正建议；医护人员通过系统实时监控患者康复情况，定期与患者进行视频交互，调整康复计划，解答康复疑问。

同时，系统根据患者的病情、康复阶段，通过 AI 推荐算法推送个性化健康宣教内容（如康复训练视频、饮食指导、用药提醒），患者可通过手机终端随时查看与学习。某康复医院的实践显示，该系统使患者居家康复训练的规范性提升 60%，康复周期缩短 25%，再入院率降低 30%；患者与医护人员的交互频率提升 40%，康复过程中的疑问得到及时解答，居家康复满意度提升 50%。此外，系统支持紧急情况一键呼救功能，当患者生命体征异常时，自动向医护人员与家属发送警报，同时传输患者实时数据，为紧急救治争取时间。

（四）智能导诊与就诊全流程交互

在院内就诊场景中，基于 AI+5G 构建智能导诊与就诊全流程交互系统，优化患者就诊体验，减少排队等待时间。患者通过医院入口的智能导诊终端或手机小程序，输入症状信息或进行语音描述，AI 模型通过症状匹配算法，精准推荐

就诊科室与医生；系统结合实时就诊量数据，为患者推荐最优就诊时间，支持在线预约挂号。就诊过程中，患者通过手机终端实时查看挂号排队进度、检查预约时间，接收医生叫号提醒；通过 5G 网络实现电子病历、检查报告的实时查询与共享，避免纸质单据丢失。

检查完成后，AI 模型快速分析检查数据，生成初步报告并推送至患者终端，同时提醒患者复诊时间；患者可通过系统在线咨询医生报告解读，避免二次到院。某三甲医院的实践显示，该系统使患者平均就诊时间从 120 分钟缩短至 60 分钟以内，挂号排队等待时间缩短 50%，检查预约时间缩短 40%，患者就诊满意度提升 35%。此外，系统支持多语言交互功能，适配不同语言背景的患者，提升医疗服务的包容性。

三、交互系统的核心架构与关键技术实现

（一）总体架构设计

智能医患交互系统采用“终端交互层-5G 传输层-边缘计算层-AI 智能交互层-应用层”五层架构，各层级协同实现多场景医患交互的智能化与体验优化。终端交互层涵盖患者终端（手机、平板、可穿戴设备）、医护终端（移动 PDA、电脑）、公共终端（智能导诊终端、病房交互平板）等，支持语音、视频、触控、手势等多模态交互方式；5G 传输层构建高速、低时延、高可靠的传输网络，实现交互数据的实时传输与多终端协同；边缘计算层部署在医院本地或区域边缘节点，提供数据预处理、实时交互分析、本地缓存等能力，提升交互响应速度与可靠性；AI 智能交互层集成语音识别引擎、NLP 处理引擎、计算机视觉引擎、推荐算法引擎等核心组件，实现交互数据的智能分析与精准响应；应用层面向远程问诊、智慧病房、居家康复、智能导诊等不同场景，提供个性化的交互服务与管理功能。

（二）关键技术实现

多模态交互融合技术：集成语音、视频、触控、手势等多模态交互方式，通过深度学习算法实现多模态交互数据的融合分析与精准识别；采用 WebRTC 协议实现端到端实时音视频交互，支持 UDP/TCP 自适应切换，在弱网环境下自动调整视频分辨率与帧率，保障交互流畅性。例如，通过 AI 算法实现语音交互与手势交互的协同，患者可同时通过语音与手势向系统发出指令，提升交互的便捷性。

AI 智能响应与个性化推荐技术：基于海量医患交互数据与医疗知识库，训练 NLP 模型实现医疗术语的精准识别、语义理解与意图判断，提升交互响应的准确性；采用协同过滤与内容推荐相结合的算法，根据患者的病情、诊疗历史、交互习惯，精准推送个性化的健康宣教内容、诊疗建议、预约提醒等信息。同时，通过用户行为分析，持续优化推荐算法，提升个性化服务质量。

隐私保护与安全交互技术：构建“端 - 边 - 云”全链路安全防护体系，终端层采用设备身份认证、数据采集加密技术；传输层采用 5G 加密传输、TLS1.3 加密等技术，防止交互数据被窃取或篡改；边缘与云端采用访问控制、权限管理、数据脱敏等技术，保障患者隐私数据安全。在远程探视、视频问诊等场景中，采用 AI 隐私遮挡技术，自动模糊患者面部、床号、病历等敏感信息，符合医疗数据安全合规要求。^①

跨系统协同与数据互通技术：通过标准化 API 接口，实现智能医患交互系统与医院现有信息系统（HIS、EMR、PACS）的无缝对接，实现患者诊疗数据、预约数据、交互数据的实时共享；采用分布式数据存储技术，实现交互数据的安全存储与快速检索，支持交互记录的全程追溯，为医疗纠纷取证提供支撑。

四、应用挑战与优化方向

（一）核心挑战

技术层面，多模态交互的融合精度有待提升，不同交互方式之间的协同性不足；AI 模型对复杂医疗场景、罕见病症状的理解与响应能力有限；5G 网络在部分偏远地区、医院地下楼层等场景的覆盖不足，影响交互稳定性。用户层面，老年患者等群体对智能交互设备的操作熟练度不足，交互界面的易用性有待优化；患者对智能交互系统的隐私保护信任度不足，影响系统的推广应用。应用层面，智能交互系统与医院现有信息系统的协同联动不足，数据互通存在壁垒；个性化交互服务的精准度有待提升，难以完全匹配不同患者的需求。

（二）优化方向

技术优化方面，加强多模态交互融合算法的研发，提升不同交互方式的协同性与识别精度；通过迁移学习、多中心数据训练等方式，提升 AI 模型对复杂医

① 王映涛. 人工智能驱动医院信息化建设的现状及管理策略 [J]. 数字技术与应用, 2025, 43 (02): 7-9.

疗场景、罕见病的适配能力；优化 5G 网络覆盖方案，采用小基站、信号增强器等设备，提升偏远地区与复杂环境的网络稳定性。用户优化方面，优化智能交互界面设计，采用简洁直观的操作流程，增加语音引导、一键呼叫等便捷功能，适配老年患者等群体的需求；加强隐私保护技术的宣传与应用，提升患者对系统的信任度。

应用优化方面，推动智能交互系统与医院现有信息系统的深度融合，建立统一的数据共享平台；加强用户行为分析，优化个性化推荐算法，提升个性化服务的精准度；开展多中心临床应用试点，积累应用经验，持续优化系统功能与交互体验；加强医护人员与患者的系统操作培训，提升系统的落地效果与推广应用范围。

第六章 区块链技术在医疗信息安全管理中的创新应用研究

第一节 区块链原理与医疗数据安全需求匹配

一、区块链核心技术原理解析

（一）区块链基础架构与核心组件

区块链是一种基于分布式账本技术的去中心化信任体系，其基础架构从上至下可分为应用层、合约层、共识层、网络层和数据层五个核心层级，各层级协同实现数据的可信存储与高效流转。应用层作为用户交互入口，涵盖医疗数据共享平台、电子病历管理系统等具体应用场景；合约层通过智能合约实现业务逻辑的自动化执行，无需第三方干预即可完成预设规则的触发与落地；共识层是区块链信任机制的核心，通过共识算法（如工作量证明 PoW、权益证明 PoS、实用拜占庭容错 PBFT 等）实现分布式节点间的状态同步与数据一致性验证；网络层依托 P2P 对等网络技术，实现节点间的信息传输与数据同步，保障网络的去中心化特性；数据层采用链式区块结构存储数据，每个区块包含区块头、交易数据和时间戳等核心信息，通过密码学哈希函数实现区块间的关联，确保数据的不可篡改。

区块链的核心组件包括分布式节点、哈希函数、非对称加密、智能合约等。分布式节点是区块链网络的基础单元，各节点独立存储完整账本，不存在中心化控制节点，有效避免了单点故障与数据篡改风险；哈希函数（如 SHA-256）具备单向性、抗碰撞性等特性，可将任意长度的输入数据转化为固定长度的哈希值，用于区块标识与数据完整性验证；非对称加密技术通过公钥与私钥的配对使用，实现数据的加密传输与身份认证，公钥可公开用于数据加密与身份验证，私钥由用户专属保管用于数据解密与数字签名；智能合约是基于可编程代码的自动化合约，当预设条件满足时自动执行相应操作，为医疗数据的共享与交互提供标准化、自动化的规则支撑。

（二）区块链核心特性与技术优势

区块链具备去中心化、不可篡改、透明可追溯、可信协同等核心特性，这些特性共同构成了其在数据安全领域的技术优势。去中心化特性通过分布式节点的协同运作，消除了中心化服务器的控制依赖，降低了因中心化节点故障、被攻击或人为操作失误导致的数据安全风险；不可篡改特性源于链式区块结构与哈希加密机制，一旦数据被写入区块并同步至各节点，任何节点试图修改数据都会导致哈希值变化，且需获得全网多数节点的验证通过，在实际应用中几乎无法实现，确保了数据的完整性与真实性；透明可追溯特性使得区块链上的所有交易数据与操作记录都可被全网节点查询，且每个数据都带有唯一的时间戳与节点签名，可实现数据全生命周期的追溯，便于责任认定与审计监督；可信协同特性基于密码学技术与共识机制，无需依赖第三方信任机构，即可实现分布式节点间的安全数据交互与业务协同，降低了信任成本。

二、医疗数据安全核心需求分析

（一）医疗数据的类型与安全风险特征

医疗数据涵盖电子病历、医学影像、检验化验结果、基因测序数据、用药记录、患者基本信息等多种类型，按数据形态可分为结构化数据（如患者年龄、性别、诊疗编码）、半结构化数据（如病历文书）和非结构化数据（如CT影像、病理切片）。医疗数据具有高敏感性、高价值性、多主体共享需求等特点，使其面临诸多安全风险。从数据流转全流程来看，风险主要体现在数据采集阶段的源头伪造风险、数据传输阶段的窃取与篡改风险、数据存储阶段的泄露与丢失风险、数据共享阶段的滥用与越权访问风险。例如，电子病历数据在跨科室、跨医院共享过程中，可能被非法拦截篡改，导致诊疗决策失误；患者基因数据等敏感信息若发生泄露，可能引发隐私侵犯、基因歧视等问题；中心化存储的医疗数据还面临服务器被攻击导致大规模数据泄露的风险。^①

（二）医疗数据安全的核心需求维度

结合医疗数据的特性与风险特征，其安全管理核心需求可归纳为数据完整性、数据保密性、身份真实性、操作可追溯性、共享可控性五个维度。数据完整性需

① 刘峰. 区块链技术在医院管理信息化中的应用[J]. 医疗装备, 2023, 36 (09): 33-36.

求要求医疗数据在采集、传输、存储、共享全流程中不被篡改、不丢失，确保数据能够真实反映患者的诊疗情况，为临床决策提供可靠依据；数据保密性需求要求敏感医疗数据仅能被授权主体访问，防止数据泄露与非法滥用，保障患者隐私；身份真实性需求要求对医疗数据的访问主体（如医护人员、患者、科研人员）进行严格身份认证，避免非法主体冒充访问；操作可追溯性需求要求对医疗数据的所有操作（如查询、修改、共享）进行完整记录，实现操作行为的全程追溯，便于后续审计与责任认定；共享可控性需求要求在满足医疗协作、科研创新等数据共享需求的同时，实现对数据共享范围、共享权限的精准控制，确保数据在可控范围内流转。

三、区块链原理与医疗数据安全需求的适配性分析

（一）技术特性与安全需求的精准匹配

区块链的核心技术特性与医疗数据安全的核心需求形成精准适配，为医疗信息安全管理提供了全新的技术支撑。区块链的不可篡改特性通过链式区块结构与哈希加密机制，确保医疗数据一旦写入便无法被非法篡改，精准匹配了医疗数据完整性需求；非对称加密技术与隐私保护机制可实现敏感医疗数据的加密存储与传输，仅授权主体可通过私钥解密访问，有效保障了数据保密性；区块链的身份认证机制基于公钥密码学，通过数字签名实现访问主体的身份验证，确保身份真实性，避免非法冒充访问；区块链上的所有操作都带有时间戳与节点签名，形成完整的操作日志，可实现医疗数据全生命周期的追溯，满足操作可追溯性需求；智能合约与访问控制机制可对数据共享的范围、权限、期限进行精准定义与自动执行，实现数据共享的可控性，平衡数据共享与隐私保护的需求。

（二）区块链在医疗数据安全中的应用优势

相较于传统的医疗信息安全管理技术（如中心化防火墙、加密存储、访问控制列表等），区块链技术具有显著应用优势。传统中心化安全管理模式依赖中心化服务器与第三方信任机构，存在单点故障、信任成本高、数据篡改风险等问题；而区块链的去中心化特性消除了中心化依赖，各节点分布式存储账本，即使部分节点故障或被攻击，也不会影响整体数据的安全性与可用性。传统技术难以实现跨机构数据共享中的可信协同，不同医院、不同机构间存在数据壁垒；区块链通过分布式共识机制与智能合约，可实现跨机构间的可信数据交互，无需依赖第三

方中介，降低了跨机构协作的信任成本。此外，区块链的操作可追溯性使得医疗数据的所有操作都可被全程记录追溯，相较于传统审计方式，更具透明度与可靠性，便于及时发现并处理非法操作行为。

第二节 基于区块链的医疗数据可信共享与隐私保护机制

一、医疗数据可信共享的核心痛点与区块链解决方案框架

（一）医疗数据可信共享的核心痛点

当前医疗数据共享面临诸多核心痛点，制约了医疗协作与科研创新的发展。一是信任缺失问题，不同医疗机构、科研机构间缺乏统一的信任基础，担心数据共享过程中发生数据泄露、篡改或滥用，导致跨机构数据共享意愿低下；二是数据壁垒问题，各医疗机构的数据多存储在独立的中心化系统中，数据格式不统一、接口不兼容，且受限于隐私保护法规与机构利益，难以实现数据的有效流通共享；三是权限管控问题，跨机构数据共享过程中，难以对数据访问权限进行精准控制，存在越权访问、数据滥用的风险；四是责任认定问题，数据共享过程中若发生数据安全事件，由于操作记录不完整、不透明，难以明确责任主体，导致追责困难。

（二）区块链驱动的医疗数据可信共享解决方案框架

基于区块链技术构建医疗数据可信共享解决方案框架，整体可分为数据接入层、区块链核心层、智能合约层、应用服务层四个层级。数据接入层负责将不同医疗机构的医疗数据（电子病历、影像数据、检验结果等）进行标准化处理，通过数据加密、格式转换等技术，将数据接入区块链网络，同时保障数据接入过程的安全性及完整性；区块链核心层依托分布式账本、共识机制、加密技术等核心组件，实现医疗数据的可信存储、操作记录的全程追溯与节点间的状态同步；智能合约层通过可编程智能合约定义数据共享的规则（如共享主体、共享范围、共享期限、访问权限等），实现数据共享的自动化、标准化执行；应用服务层面向临床协作、科研创新、公共卫生等具体应用场景，提供数据共享查询、权限管理、审计监督等服务。该框架通过区块链的去中心化信任机制，消除跨机构数据共享的信任壁垒；通过智能合约实现权限的精准管控，保障数据共享的可控性；通过分布式账本实现操作记录的全程追溯，便于责任认定。

二、基于区块链的医疗数据可信共享关键机制

（一）数据标准化接入与可信上链机制

数据标准化接入是实现跨机构数据共享的基础，通过制定统一的医疗数据接入标准（如基于 HL7 FHIR、DICOM 等医疗数据标准），对不同医疗机构的异构数据进行格式转换、字段映射，确保接入区块链的医疗数据具备一致性与可读性。可信上链机制通过数据校验、加密处理、数字签名等技术，保障医疗数据上链过程的安全性、完整性。具体流程为：医疗机构数据采集终端采集医疗数据后，首先通过本地校验模块对数据进行完整性、准确性校验；校验通过后，采用非对称加密技术对敏感数据进行加密处理；加密后的数据由医疗机构节点进行数字签名，确保数据来源的真实性；最后，通过区块链节点的共识验证，将数据写入区块链分布式账本，完成数据的可信上链。同时，为避免全量医疗数据上链导致的存储压力与隐私泄露风险，可采用“链上存证+链下存储”的模式，仅将数据的哈希值、关键元数据、操作记录等核心信息上链，原始医疗数据存储在各医疗机构的本地节点或分布式存储系统中，通过链上哈希值实现对原始数据的完整性验证。^①

（二）跨机构共识与可信协同机制

跨机构共识机制是实现不同医疗机构节点间数据一致性与信任协同的核心。针对医疗数据共享场景的特点（如数据敏感性高、交易吞吐量需求适中、响应速度要求较高），可采用改进型实用拜占庭容错（PBFT）共识算法，通过选举主节点负责交易提案，其他节点负责验证提案的有效性，当超过 2/3 的节点验证通过后，即可完成共识并将数据写入账本。该共识算法相较于 PoW、PoS 等算法，具有交易确认速度快、能耗低的优势，更适配医疗数据共享的实时性需求。可信协同机制通过智能合约定义跨机构数据共享的协作规则，实现数据共享的自动化协同。例如，当不同医院需要开展多学科会诊时，发起会诊的医院节点可通过智能合约向相关医院节点发送数据共享请求，相关医院节点通过智能合约验证请求的合法性与权限后，自动授权访问相应的医疗数据，会诊完成后，智能合约自动记录数据访问日志，并终止数据访问权限，实现跨机构会诊的可信协同。

^① 娄岚清,魏东晓,刘颖.区块链技术在医院管理中的应用分析[J].现代医院管理,2022,20(04):78-80.

（三）动态权限管控与访问审计机制

基于区块链与智能合约构建动态权限管控机制，实现对医疗数据访问权限的精准定义、动态调整与自动化执行。首先，通过智能合约定义不同访问主体（医护人员、患者、科研人员）的基础权限模板，明确不同主体可访问的数据范围与操作类型；其次，当访问主体需要访问特定医疗数据时，向区块链网络提交访问请求，智能合约自动校验访问主体的身份信息、权限等级与数据访问需求的匹配性，校验通过后授予临时访问权限；访问权限的有效期、访问次数等可通过智能合约进行精准控制，超过预设条件后自动回收权限。动态权限管控机制还支持权限的实时调整，当访问主体的身份、职责发生变化时，可通过智能合约快速更新权限配置。访问审计机制依托区块链的可追溯特性，对所有医疗数据的访问操作进行完整记录，包括访问主体、访问时间、访问数据、操作类型等信息，形成不可篡改的审计日志。审计人员可通过区块链平台实时查询审计日志，对数据访问操作进行监督检查，及时发现并处理越权访问、非法操作等问题，同时审计日志可作为责任认定的可靠依据。

三、基于区块链的医疗数据隐私保护核心技术与机制

（一）密码学技术支撑的隐私保护机制

结合多种密码学技术，构建多层次的医疗数据隐私保护机制。一是非对称加密技术，用于医疗数据的加密存储与传输，患者、医疗机构等主体通过各自的公钥与私钥实现数据的加密与解密，确保敏感数据仅能被授权主体访问；二是零知识证明技术，实现“数据可用不可见”的隐私保护目标，例如科研机构需要使用医疗数据进行研究时，无需获取原始医疗数据，通过零知识证明技术即可验证数据是否满足研究需求，同时不泄露任何敏感信息；三是同态加密技术，支持对加密后的医疗数据直接进行计算分析，无需解密，计算结果仍以加密形式存在，仅授权主体可解密获取结果，有效保障了数据在计算过程中的隐私安全；四是哈希摘要技术，对医疗数据进行哈希处理，将原始数据转化为固定长度的哈希值，仅将哈希值上链，避免原始敏感数据的公开泄露，同时可通过哈希值验证原始数据的完整性。

（二）链上链下结合的隐私保护架构

采用“链上存证+链下存储”的混合架构，平衡数据共享效率、存储成本与

隐私保护需求。链上仅存储医疗数据的关键元数据（如数据标识、数据来源、数据哈希值）、操作记录、权限配置等非敏感信息，确保数据的可追溯性与权限管控的有效性；原始医疗数据（如完整电子病历、医学影像、基因数据等）存储在各医疗机构的本地链下存储系统或分布式隐私存储节点中，链下存储系统采用加密存储技术保障数据安全，同时通过区块链上的智能合约实现对链下数据访问权限的管控。当需要访问原始医疗数据时，访问主体通过区块链平台提交访问请求，智能合约校验通过后，向链下存储系统发送授权指令，链下存储系统根据授权指令向访问主体提供加密的原始数据，访问主体通过私钥解密获取数据。该架构既避免了全量敏感数据上链导致的隐私泄露风险，又通过链上存证与权限管控保障了数据的可信共享。

（三）基于智能合约的隐私保护策略自动化执行机制

通过智能合约将隐私保护策略（如数据加密规则、访问权限规则、数据脱敏规则）进行代码化定义，实现隐私保护策略的自动化执行。例如，针对不同类型的医疗数据，通过智能合约预设不同的加密级别与脱敏规则，敏感程度高的基因数据采用高强度非对称加密与全量脱敏处理，一般诊疗数据采用对称加密与部分脱敏处理；当数据接入区块链时，智能合约自动根据数据类型执行相应的加密与脱敏操作。在数据共享过程中，智能合约自动校验访问主体的隐私保护资质，仅允许具备相应资质的主体访问特定敏感数据；同时，智能合约可对数据共享过程进行实时监控，当发现异常访问行为（如超出权限范围访问、多次访问敏感数据）时，自动触发预警机制，通知相关管理主体并采取暂停访问权限、记录违规行为等措施。此外，智能合约还可实现隐私保护策略的动态更新，当隐私保护法规、机构隐私政策发生变化时，可通过修改智能合约代码快速更新隐私保护策略，确保隐私保护机制的适应性与合规性。

四、应用实践效果与面临的挑战

（一）典型应用场景实践效果

在跨机构临床协作场景中，某区域医疗联合体基于区块链技术构建医疗数据可信共享平台，整合了区域内 10 家医疗机构的电子病历、检验化验、医学影像等数据。平台通过区块链的可信共享与隐私保护机制，实现了跨机构数据的安全共享与协同诊疗，医护人员可通过平台快速获取患者的完整诊疗数据，无需患者重

复检查,使区域内平均诊疗时间缩短 30%,重复检查率降低 25%,疑难病例会诊效率提升 40%。同时,平台通过隐私保护机制确保了患者数据的安全,未发生一起数据泄露事件,患者对数据共享的信任度提升 60%。在医疗科研数据共享场景中,某科研机构与多家医院合作构建基于区块链的科研数据共享平台,通过零知识证明、同态加密等隐私保护技术,实现了科研数据的“可用不可见”,科研人员无需获取原始患者数据即可开展研究,既保障了患者隐私,又提升了科研数据的共享效率,使科研项目的数据分析周期缩短 45%,研究成果产出速度提升 35%。

（二）面临的核心挑战

尽管区块链技术在医疗数据可信共享与隐私保护领域具有显著优势,但仍面临诸多核心挑战。技术层面,区块链网络的交易吞吐量与响应速度有待提升,难以满足大规模医疗数据实时共享的需求;不同区块链平台间的互操作性不足,导致跨平台数据共享困难;链下存储与链上数据的一致性同步机制尚不完善,存在数据篡改风险。管理层面,缺乏统一的区块链医疗数据共享标准与规范,不同医疗机构的数据格式、接口不统一,影响数据共享的效率;跨机构、跨区域的区块链节点协同管理机制不完善,导致节点维护、共识验证等工作难以高效推进。合规层面,区块链技术的去中心化特性与现有医疗数据管理法规(如数据主权归属、跨境数据流动)存在适配性问题;智能合约的法律地位尚未明确,若发生合约执行纠纷,难以进行法律追责。此外,区块链技术的部署与运维成本较高,对医疗机构的技术实力与资金投入提出了较高要求,限制了其在中小医疗机构的推广应用。

（三）优化方向

技术优化方面,研发高性能区块链技术,通过分片技术、侧链技术、共识算法优化等方式,提升区块链网络的交易吞吐量与响应速度;制定区块链医疗数据共享的技术标准与接口规范,提升不同区块链平台间的互操作性;完善链下存储与链上数据的一致性同步机制,通过加密校验、实时监控等技术,确保数据的安全性、完整性。管理优化方面,建立跨机构、跨区域的区块链节点协同管理机制,明确各节点的职责与权利,提升节点管理效率;加强医疗机构的技术培训与人才培养,提升其区块链技术的应用与运维能力;推动区块链技术与现有医疗信息系统的深度融合,降低部署与运维成本。合规优化方面,加快完善区块链医疗数据管理相关法律法规,明确数据主权归属、智能合约的法律地位等关键问题;建立

区块链医疗数据共享的合规评估机制，确保技术应用符合现有法规要求；加强国际间的法规协同，推动跨境医疗数据的合法合规共享。

第三节 区块链在药品全生命周期溯源与 医疗供应链管理中的应用

一、药品全生命周期溯源的核心痛点与区块链技术适配性

（一）药品全生命周期溯源核心痛点

药品从研发生产、流通运输到终端使用的全生命周期涉及药企、经销商、物流企业、医疗机构、监管部门等多个主体，当前溯源体系存在诸多核心痛点。一是溯源信息碎片化，各主体采用独立的中心化溯源系统，数据格式不统一、接口不兼容，形成“信息孤岛”，无法实现全链条信息贯通，出现药品质量问题时难以快速追溯源头；二是数据可信度不足，中心化溯源系统易受人为操作干预，存在数据篡改、伪造风险，例如部分不良商家通过篡改生产日期、有效期等信息销售过期药品；三是责任认定困难，药品流转环节多，各主体间信息传递不透明，出现质量问题时相互推诿，难以明确责任主体；四是监管效率低下，监管部门需跨多个系统采集溯源数据，信息获取不及时、不全面，无法实现对药品全生命周期的实时监管。

（二）区块链技术与药品溯源需求的适配性

区块链的核心特性与药品全生命周期溯源需求形成精准适配，为解决溯源痛点提供了技术支撑。区块链的不可篡改特性通过链式区块结构与哈希加密机制，确保药品溯源信息一旦写入便无法被非法篡改，保障了溯源数据的真实性与完整性；去中心化特性消除了对中心化溯源系统的依赖，各参与主体作为分布式节点共同维护溯源账本，实现溯源信息的多节点共享与协同验证，打破“信息孤岛”；透明可追溯特性使得药品从生产到使用的全流程信息可被全程追溯，每个流转环节都带有时间戳与节点签名，便于快速定位问题环节与责任主体；可信协同特性基于密码学技术与共识机制，实现各参与主体间的可信数据交互，无需依赖第三方中介，提升溯源信息传递效率。

二、基于区块链的药品全生命周期溯源体系构建

（一）溯源体系架构设计

基于区块链的药品全生命周期溯源体系采用“终端感知层-数据接入层-区块链核心层-应用服务层”四层架构。终端感知层部署在药品生产、流通、使用各环节，涵盖药品生产线传感器、RFID 标签、温湿度监测设备、手持扫码终端等，负责采集药品生产信息、流转信息、环境信息等多源数据；数据接入层通过数据标准化处理、加密传输等技术，将各终端采集的异构数据转化为统一格式，经节点验证后接入区块链网络，保障数据接入的安全性与一致性；区块链核心层依托分布式账本、共识机制、非对称加密等核心组件，实现溯源数据的可信存储、全链同步与不可篡改，采用改进型 PBFT 共识算法提升数据写入与验证效率，适配药品高频流转场景；应用服务层面向药企、医疗机构、监管部门、患者等不同用户，提供溯源查询、责任认定、监管预警、数据分析等个性化服务。^①

（二）全生命周期溯源关键流程实现

生产环节溯源：药企在药品生产完成后，通过终端设备采集药品名称、规格、批号、生产日期、有效期、原料来源、生产工艺等信息，生成唯一的药品溯源码（如基于 RFID 的唯一标识），采用非对称加密技术对信息进行加密处理后，由药企节点进行数字签名并上传至区块链，完成药品生产信息的可信上链，实现“一物一码”溯源基础。流通环节溯源：药品出厂后，经销商、物流企业通过扫码终端读取药品溯源码，采集药品出库时间、运输车辆信息、温湿度数据、中转节点、入库时间等流转信息，经节点验证后写入区块链；运输过程中，温湿度监测设备实时采集环境数据并上传至区块链，若出现温湿度超标等异常情况，系统自动触发预警机制，通知相关主体及时处理。使用环节溯源：医疗机构接收药品时，通过扫码验证药品溯源信息的真实性与完整性，采集入库时间、领用科室、使用患者等信息并上链；患者可通过医院终端或手机小程序扫描药品溯源码，查询药品全生命周期信息，确保用药安全。监管环节溯源：监管部门通过区块链平台实时获取药品全流程溯源数据，开展数据分析与风险监测，对异常流转、信息篡改等违规行为进行实时预警，实现精准监管。

① 邢昊, 赵飞. 区块链技术在医疗医药领域应用困境及改进策略的研究 [J]. 中国数字医学, 2025, 20 (02): 50-56.

三、区块链驱动的医疗供应链管理优化实践

（一）医疗供应链管理核心痛点

医疗供应链涵盖药品、医疗器械、耗材等医疗物资的采购、仓储、运输、配送、使用全流程，涉及供应商、医疗机构、物流企业、医保部门等多个主体，当前管理模式存在诸多痛点。一是供应链协同效率低，各主体间信息不对称、沟通成本高，采购订单、物流信息、验收单据等信息传递滞后，导致物资供应不及时，影响临床诊疗工作；二是库存管理不合理，医疗机构缺乏实时、精准的供应链数据支撑，难以准确预测物资需求，易出现库存积压或短缺问题，增加运营成本；三是资金结算周期长，采购合同执行、发票审核、医保报销等环节流程繁琐，信息不透明，导致资金结算周期长，影响供应链资金流转效率；四是质量管控难度大，医疗物资尤其是高值耗材的来源、流转、使用等信息难以全程追溯，存在假冒伪劣、以次充好等质量风险。

（二）区块链在医疗供应链管理中的优化应用

供应链协同管理优化：基于区块链构建医疗供应链协同平台，整合供应商、医疗机构、物流企业等主体的信息资源，实现采购订单、物流轨迹、验收结果等信息的实时共享与可信交互。通过智能合约定义各主体的协作规则，当医疗机构提交采购订单后，智能合约自动校验供应商资质与物资库存，触发订单确认、物流调度等自动化流程；物流企业实时上传物资运输信息，医疗机构可通过平台实时跟踪物资位置与状态，实现供应链全流程可视化协同，提升供应效率。例如，某区域医疗联合体构建的区块链供应链协同平台，使医疗物资采购响应时间缩短 40%，物资供应延迟率降低 35%。

智能库存管理优化：结合区块链与物联网技术，实现医疗物资库存的实时监控与智能管理。在仓储环节部署 RFID 传感器与库存监测设备，实时采集物资库存数量、存放位置、有效期等信息并上传至区块链；通过 AI 算法分析历史使用数据、临床需求数据，精准预测物资需求，智能生成采购建议；当物资库存低于预设阈值或临近有效期时，系统自动触发预警机制，通知相关部门及时采购或处理，避免库存短缺或过期浪费。某三甲医院的实践显示，应用该系统后，医疗物资库存积压率降低 28%，短缺率降低 32%，库存管理成本降低 25%。

供应链质量管控优化：将区块链溯源技术延伸至医疗耗材、医疗器械等物资的全生命周期管理，实现物资来源可查、去向可追、责任可究。供应商在物资出

厂时，将生产信息、质量检测报告等数据上链，生成唯一溯源码；物资流转过程中，各环节实时上传流转信息；医疗机构验收时，通过扫码验证物资质量信息的真实性与完整性，确保物资质量合格。监管部门通过区块链平台实时监控供应链质量数据，对质量异常物资进行快速追溯与处置，提升质量管控效率。

四、应用效果与面临的挑战

（一）典型应用效果

某省药品监督管理局联合药企、医疗机构构建基于区块链的药品溯源平台，覆盖全省 500 余家医疗机构、200 余家药企，实现了药品全生命周期溯源管理。平台运行后，药品质量问题追溯时间从平均 72 小时缩短至 6 小时以内，假药、劣药流入市场的风险降低 60%；患者用药安全信任度提升 55%，监管部门执法效率提升 45%。在医疗供应链管理领域，某大型医疗集团应用区块链供应链协同平台后，医疗物资采购周期缩短 35%，库存周转率提升 30%，资金结算周期缩短 25%，供应链运营成本降低 20%，有效提升了供应链管理的精细化水平。

（二）核心挑战与优化方向

核心挑战：技术层面，区块链网络交易吞吐量有限，难以适配医疗物资高频流转场景的实时数据写入需求；终端设备兼容性不足，不同品牌的 RFID 设备、传感器数据格式不统一，影响数据采集效率；链上链下数据同步机制不完善，存在数据延迟或不一致风险。管理层面，缺乏统一的区块链医疗供应链管理标准与规范，各主体数据共享意愿参差不齐；跨主体协同管理机制不完善，责任划分与利益分配不明确。合规层面，区块链溯源数据的法律地位尚未明确，作为监管执法与责任认定依据的适用性有待验证；医疗供应链数据包含商业秘密与敏感信息，数据共享与隐私保护的平衡难度大。

优化方向：技术优化方面，采用分片技术、侧链技术提升区块链网络吞吐量；制定终端设备数据接口标准，提升设备兼容性；完善链上链下数据同步机制，通过加密校验与实时监控确保数据一致性。管理优化方面，推动制定区块链医疗供应链管理行业标准；建立跨主体协同管理机制，明确各主体职责与利益分配；加强主体间的沟通协作，提升数据共享意愿。合规优化方面，加快完善区块链数据相关法律法规，明确溯源数据的法律地位；采用隐私计算技术实现敏感数据“可用不可见”，平衡数据共享与隐私保护需求。

第四节 智能合约在医疗结算中的应用实践

一、医疗结算的核心痛点与智能合约技术适配性

（一）医疗结算核心痛点

医疗结算涉及患者、医疗机构、医保部门、商业保险公司等多个主体，涵盖门诊结算、住院结算、医保报销、商业保险理赔等多个场景，当前结算模式存在诸多痛点。一是结算流程繁琐，传统医疗结算需经过诊疗记录核对、费用明细统计、发票开具、医保审核、资金拨付等多个环节，流程繁琐、周期长，增加了各主体的时间成本与人力成本；二是信息不对称，各主体间结算数据格式不统一、信息传递不透明，导致医保审核、保险理赔过程中频繁出现数据核对不一致问题，影响结算效率；三是资金结算延迟，医保报销、商业保险理赔等结算场景中，由于审核流程复杂、信息传递滞后，资金拨付周期长，影响医疗机构资金流转与患者就医体验；四是风险管控难度大，结算过程中存在虚假报销、过度医疗、费用篡改等违规风险，传统结算模式难以实现实时监管与风险预警。

（二）智能合约与医疗结算需求的适配性

智能合约的自动化、透明化、不可篡改特性与医疗结算的核心需求高度适配，为优化结算流程提供了全新解决方案。智能合约的自动化执行特性可将医疗结算的规则（如医保报销比例、缴费标准、理赔条件等）代码化，当满足预设结算条件时自动触发结算流程，无需人工干预，大幅简化结算流程、缩短结算周期；透明化特性确保结算规则、费用明细、审核结果等信息在各主体间实时共享，避免信息不对称导致的核对纠纷；不可篡改特性保障结算数据与流程记录的真实性和完整性，有效防范虚假报销、费用篡改等违规风险；此外，智能合约与区块链的结合可实现结算全流程的可追溯，便于后续审计与责任认定，提升结算风险管控能力。

二、基于智能合约的医疗结算体系架构与核心流程

（一）结算体系架构设计

基于智能合约的医疗结算体系采用“数据采集层 - 区块链核心层 - 智能合约层 - 应用服务层”四层架构。数据采集层通过标准化接口对接医院 HIS 系统、电

子病历系统、医保系统、商业保险系统等，采集患者诊疗记录、费用明细、医保政策、保险条款等结算相关数据，经数据清洗、加密处理后接入区块链网络；区块链核心层负责结算数据的可信存储、全链同步与不可篡改，保障结算数据的安全性、完整性；智能合约层是体系核心，包含医保结算合约、商业保险理赔合约、门诊/住院结算合约等多种类型合约，通过代码定义结算规则、触发条件、资金拨付流程等；应用服务层面向患者、医疗机构、医保部门、保险公司等主体，提供结算申请、费用查询、审核结果查看、资金到账通知等个性化服务。

（二）核心结算流程实现

门诊/住院结算流程：患者完成诊疗后，医院 HIS 系统自动采集诊疗费用明细、药品使用记录、检查项目等数据，上传至区块链网络；智能合约自动匹配对应的医保报销政策或商业保险条款，计算个人自付金额、医保报销金额、保险理赔金额；患者通过终端设备确认费用明细后，智能合约自动触发支付流程，从患者个人账户、医保账户、保险公司账户中分别扣划对应资金，完成实时结算；结算完成后，智能合约自动生成结算凭证并上链存储，供各主体查询验证。

医保报销结算流程：医疗机构提交医保报销申请后，智能合约自动校验申请材料的完整性与真实性，核对诊疗记录与费用明细是否符合医保政策；审核通过后，智能合约自动计算报销金额，触发医保资金拨付流程，将报销资金直接拨付至医疗机构账户；审核不通过时，智能合约自动生成审核意见并反馈给医疗机构，明确未通过原因。整个流程无需人工审核，大幅缩短医保报销周期。

商业保险理赔流程：患者出险后，通过终端提交理赔申请并上传诊疗记录、费用发票等材料；智能合约自动校验理赔材料的真实性与完整性，匹配保险条款中的理赔条件；符合理赔条件的，智能合约自动计算理赔金额，触发保险资金拨付流程；不符合理赔条件的，自动生成拒赔意见并反馈给患者。同时，智能合约实时同步理赔进度至各主体，提升理赔透明度。

三、智能合约在医疗结算中的典型应用场景实践

（一）医保实时结算场景

某城市医保部门联合医疗机构构建基于智能合约的医保实时结算平台，将医保报销政策代码化写入智能合约，实现门诊、住院费用的实时结算。患者在医疗机构完成诊疗后，智能合约自动匹配医保政策，计算报销金额，完成个人自付部

分与医保报销部分的实时扣款与资金划转,结算凭证实时上链存储。平台运行后,医保报销周期从平均 30 天缩短至实时完成,患者就医结算等待时间从平均 40 分钟缩短至 5 分钟以内;医疗机构医保资金回笼周期缩短 60%,财务运营效率显著提升;医保部门审核工作量减少 75%,虚假报销风险降低 50%,监管效率大幅提升。

（二）商业健康保险快速理赔场景

某商业保险公司与多家医疗机构合作,构建基于智能合约的健康保险快速理赔平台。平台通过区块链技术实现保险公司与医疗机构的数据共享,将保险条款、理赔条件代码化写入智能合约。患者在合作医疗机构诊疗后,无需提交纸质理赔材料,智能合约自动从医疗机构获取诊疗记录与费用明细,校验理赔条件并计算理赔金额,自动完成理赔资金拨付。平台运行后,商业保险理赔周期从平均 15 天缩短至 24 小时以内,理赔材料提交量减少 90%,患者理赔体验显著提升;保险公司理赔审核成本降低 65%,虚假理赔风险降低 45%,理赔效率与风险管控能力同步提升。

（三）跨区域医疗协作结算场景

某区域医疗联合体构建基于智能合约的跨区域医疗协作结算平台,实现不同医疗机构间的诊疗费用协同结算。当患者在联合体内部跨医院就诊时,智能合约自动同步患者诊疗记录与费用明细,按照预设的费用分摊规则,自动完成不同医疗机构间的费用结算与资金划转;同时,智能合约自动匹配医保政策,完成跨区域医保报销的实时结算。平台运行后,跨区域医疗协作结算周期从平均 7 天缩短至实时完成,医疗机构间费用核对纠纷减少 80%,跨区域就医患者的结算便捷性显著提升,有效促进了区域医疗资源的协同利用。

四、应用挑战与优化方向

（一）核心挑战

技术层面,智能合约代码安全性不足,存在代码漏洞、逻辑缺陷等风险,可能导致结算错误或资金损失;区块链网络交易吞吐量与响应速度有限,难以适配医疗结算高峰期的大规模并发需求;不同系统间数据接口不统一,影响结算数据的顺畅流转。法律层面,智能合约的法律地位尚未明确,其法律效力与传统纸质合同的等同性有待验证;结算过程中若出现合约执行纠纷,责任认定与法律追责难度大。管理层面,医保政策、保险条款等结算规则具有动态调整特性,智能合

约的规则更新流程复杂，难以快速适配政策变化；各主体对智能合约技术的认知与接受度不足，影响技术推广应用。

（二）优化方向

技术优化方面，建立智能合约代码审计与测试机制，引入第三方安全机构对合约代码进行全面审核，防范代码漏洞；采用高性能区块链技术提升网络吞吐量与响应速度，适配并发结算需求；制定统一的数据接口标准，实现各系统间的数据顺畅流转。法律优化方面，加快完善智能合约相关法律法规，明确其法律地位与法律效力；建立智能合约纠纷解决机制，明确责任划分标准与追责流程。管理优化方面，设计灵活的智能合约规则更新机制，支持医保政策、保险条款的快速适配；加强各主体的技术培训与认知普及，提升对智能合约技术的接受度；建立跨主体协同管理机制，保障结算体系的高效运行。

第七章 边缘计算与算力网络在医院信息化管理中的应用研究

第一节 边缘计算架构与医疗高实时性应用场景

一、边缘计算核心架构与技术特性

（一）边缘计算核心架构解析

边缘计算是一种将计算资源、存储资源和网络资源部署在靠近数据产生源头（边缘节点）的分布式计算架构，旨在减少数据传输延迟、降低核心网络带宽占用、提升数据处理效率与安全性。面向医院信息化管理场景，边缘计算架构采用“云-边-端”三级协同架构，从上至下可分为云端管理层、边缘节点层和终端感知层三个核心层级，各层级协同实现医疗数据的实时处理与服务的高效交付。

云端管理层作为架构的核心管控中枢，部署在医院数据中心或公有云平台，主要负责全局资源调度、边缘节点管理、数据汇总分析、应用程序下发等核心功能。通过算力网络调度平台，云端可实时监控各边缘节点的资源占用情况（CPU、内存、存储、带宽），根据医疗业务需求动态分配算力资源，实现全局算力的优化配置；同时，云端负责对边缘节点上传的海量医疗数据进行深度分析与挖掘，为医院管理决策、临床科研等提供数据支撑。

（二）边缘计算核心技术特性

终端感知层是数据产生的源头，涵盖各类医疗终端设备与传感器，包括生命体征监测设备、手术机器人、医学影像设备、移动医护终端、急救车车载设备、智能病房终端等。终端感知层负责采集患者生命体征数据、诊疗操作数据、设备运行数据等多源医疗数据，通过本地网络与边缘节点建立连接，将数据传输至边缘节点进行实时处理，同时接收边缘节点下发的控制指令与服务响应。

边缘节点层是架构的核心处理单元，部署在医院各科室楼层、门诊楼、住院楼、急救中心等靠近医疗终端的位置，涵盖边缘服务器、边缘网关、边缘路由器

等设备。边缘节点层具备本地数据处理、存储、网络转发等核心能力，可对终端感知层采集的医疗数据进行实时预处理与分析，快速响应终端设备的服务请求；同时，边缘节点与云端保持实时数据同步，接受云端的统一管理与调度，在网络中断等极端情况下，可独立运行保障核心医疗业务的连续性。

边缘计算的核心技术特性与医院信息化管理的高实时性、高可靠性需求高度适配，主要体现在低延迟、高可靠、高带宽、本地自治、安全可控五个方面。低延迟特性：边缘节点靠近数据源头，医疗数据无需传输至远端云端即可完成处理，数据传输与处理延迟可降低至毫秒级，能够满足医疗业务对实时性的严苛要求；高可靠特性：通过多边缘节点冗余部署与“云-边”协同备份机制，即使单个边缘节点故障，也可快速切换至其他节点或云端，保障医疗服务的连续性；高带宽特性：边缘节点对本地医疗数据进行预处理与过滤，仅将关键数据上传至云端，可大幅降低核心网络带宽占用，提升数据传输效率；本地自治特性：边缘节点具备独立的计算与存储能力，在网络中断或不稳定时，可独立运行核心医疗业务，避免因网络问题导致医疗服务中断；安全可控特性：医疗数据在本地边缘节点完成处理，减少了数据跨网络传输的风险，同时边缘节点具备本地数据加密、访问控制等安全能力，可有效保障医疗数据的隐私与安全。

二、医院高实时性应用场景特征与需求

（一）医院高实时性应用场景核心特征

医院高实时性应用场景主要集中在临床诊疗、急救救援、智能病房管理等核心业务环节，具有数据产生量大、实时处理需求高、服务连续性要求严、数据安全性敏感等核心特征。从数据特性来看，此类场景产生的医疗数据多为实时流式数据（如患者心率、血压等生命体征数据），数据产生频率高、时效性强，需在极短时间内完成处理与响应；从服务需求来看，此类场景直接关系到患者生命安全，要求医疗服务具备毫秒级响应能力，服务中断可能导致严重的医疗风险；从安全需求来看，场景涉及的患者生命体征、诊疗记录等数据属于高度敏感信息，需保障数据传输与处理过程的安全性及隐私性。

（二）高实时性应用场景核心需求

结合高实时性应用场景的特征，其核心需求可归纳为实时数据处理、低延迟服务响应、连续服务保障、数据安全隐私四个维度。实时数据处理需求要求系统

能够快速采集、清洗、分析海量实时医疗数据，提取关键信息并生成决策支撑；低延迟服务响应需求要求系统从数据产生到服务响应的全流程延迟控制在毫秒级，确保医疗干预的及时性；连续服务保障需求要求系统具备高可靠性与容错能力，能够应对网络中断、设备故障等突发情况，保障医疗服务不中断；数据安全隐私需求要求系统采用严格的安全防护措施，防止医疗数据泄露、篡改或滥用，符合医疗数据安全合规要求。

三、边缘计算架构与医疗高实时性场景的适配性应用

（一）手术室实时诊疗场景

手术室是医院高实时性需求最为严苛的场景之一，手术过程中需实时监测患者生命体征（心率、血压、血氧饱和度、体温等）、手术设备运行状态（如手术机器人、麻醉机、呼吸机等），并根据监测数据实时调整手术方案。边缘计算架构在手术室场景的应用的具体实现为：在手术室部署边缘节点，连接手术室内的生命体征监测设备、手术机器人、影像设备等终端；终端设备实时采集患者生命体征数据与设备运行数据，传输至本地边缘节点进行毫秒级处理；边缘节点通过AI算法对数据进行实时分析，若发现患者生命体征异常或设备运行故障，立即触发预警机制，向手术医生、麻醉师推送预警信息，并同步至手术室监控中心；同时，边缘节点将关键诊疗数据实时上传至云端，供术后复盘与科研分析。边缘计算的低延迟特性确保了手术过程中异常情况的及时发现与处置，高可靠特性保障了手术数据的连续采集与处理，为手术安全提供了有力支撑。

（二）急诊急救与院前急救协同场景

急诊急救与院前急救协同场景要求实现“院前 - 院中”数据实时同步与服务快速响应，为危重患者争取救治时间。边缘计算架构通过“急救车边缘节点 + 医院急诊边缘节点”的协同部署，实现场景适配：急救车配备移动边缘节点，连接车载生命体征监测设备、高清视频采集设备等终端，实时采集患者生命体征数据、现场影像数据；移动边缘节点对数据进行实时预处理与加密，通过5G网络将数据传输至医院急诊边缘节点；医院急诊边缘节点接收数据后，快速解析并推送至急诊医生终端，同时自动调用医院HIS系统、电子病历系统相关数据，为医生提前制定救治方案提供支撑；患者到达医院后，急诊边缘节点将院前急救数据与院内诊疗数据无缝对接，实现救治流程的高效衔接。边缘计算的低延迟与高带宽特

性保障了院前 - 院中数据的实时传输，本地自治特性确保了在偏远地区网络信号不稳定时，急救车移动边缘节点可本地存储关键数据，网络恢复后快速同步，避免数据丢失。

（三）智能病房实时监测场景

智能病房场景需实时监测住院患者生命体征、病房环境参数（温湿度、空气质量、光照等），并实现患者与医护人员的快速交互。边缘计算架构在该场景的应用为：在病房楼层部署边缘节点，连接病房内的智能病床、生命体征监测手环、环境传感器、病房交互终端等设备；终端设备实时采集患者生命体征数据与环境数据，传输至楼层边缘节点进行实时处理；边缘节点通过预设阈值与 AI 算法分析数据，若发现患者生命体征异常（如心率过快、血压骤降）或环境参数超标，立即触发声光预警，并向医护人员移动终端推送预警信息；同时，边缘节点支持患者通过病房交互终端发起一键呼叫、诊疗咨询等请求，快速响应并转接至相关医护人员。边缘计算的本地处理能力减少了数据传输延迟，确保了患者异常情况的及时预警与处置；多边缘节点冗余部署保障了病房监测服务的连续性，提升了患者住院体验与医疗安全。

（四）医学影像实时处理场景

医学影像（如 CT、MRI、超声等）检查场景需对海量影像数据进行实时处理与分析，为医生快速提供诊断依据。传统影像处理模式依赖云端服务器，数据传输与处理延迟较高，影响诊断效率。边缘计算架构的应用优化了这一流程：在影像科部署边缘节点，连接 CT、MRI 等影像设备；影像设备采集的影像数据实时传输至本地边缘节点，边缘节点通过轻量化 AI 算法对影像数据进行实时预处理（如降噪、增强、分割）与初步分析，提取病灶特征并标记可疑区域；处理后的影像数据与分析结果同步至医生诊断终端，供医生快速查看与精准诊断；同时，边缘节点将原始影像数据与诊断结果上传至云端进行长期存储与深度分析。边缘计算的本地实时处理能力将影像数据处理延迟从秒级缩短至毫秒级，大幅提升了影像诊断效率，为急重症患者的快速诊断与治疗提供了支撑。

第二节 边缘计算支撑的医疗实时数据处理与低延迟医疗服务

边缘计算通过“终端感知+边缘汇聚”的模式，构建多源医疗数据实时采集与预处理机制。在数据采集环节，边缘节点通过标准化接口（如 HL7 FHIR、DICOM、MQTT 等）连接各类医疗终端设备与传感器，支持对结构化数据（如生命体征数值）、半结构化数据（如诊疗记录）、非结构化数据（如医学影像、语音指令）的多模态数据采集；同时，边缘节点具备数据采集权限管控功能，仅采集经授权的医疗数据，保障数据采集的合规性。在数据预处理环节，边缘节点对采集的原始数据进行实时清洗（去除噪声、填补缺失值、纠正异常值）、格式转换（将异构数据转化为统一格式）、数据压缩（减少数据体积，降低传输带宽占用）等处理；针对高维度医疗数据（如医学影像），边缘节点采用轻量化特征提取算法，提取关键特征数据，为后续分析处理提供支撑。通过实时采集与预处理，边缘计算确保了医疗数据的及时性、准确性与可用性，为后续实时分析与服务响应奠定基础。

一、边缘计算驱动的医疗实时数据处理机制

（一）多源医疗数据实时采集与预处理机制

边缘计算通过算力网络实现各边缘节点间、边缘节点与云端间的医疗数据实时共享与协同交互。在边缘节点间协同方面，同一医院内不同科室的边缘节点通过本地算力网络建立连接，实现跨科室医疗数据的实时共享。例如，急诊边缘节点可将院前急救数据实时共享至影像科、检验科边缘节点，提前触发影像检查、化验检测等流程，提升救治效率；在“云-边”协同方面，边缘节点与云端通过高速网络实现数据实时同步，云端将医疗政策、诊疗规范、AI 模型参数等数据下发至边缘节点，边缘节点将本地处理结果、设备运行状态等数据上传至云端，实现全局协同。同时，边缘计算采用数据加密传输、访问控制、数据脱敏等安全技术，保障数据共享过程的安全性及隐私性。通过实时共享与协同交互，边缘计算打破了医疗数据的“信息孤岛”，提升了医院各科室间的协同诊疗效率。

（二）实时数据分布式分析与智能决策机制

边缘计算采用“本地边缘分析+云端协同分析”的分布式分析模式，实现医疗数据的实时分析与智能决策。在本地边缘分析环节，边缘节点部署轻量化 AI

模型（如轻量化神经网络、决策树模型等），对预处理后的实时医疗数据进行实时分析，快速生成初步决策结果。例如，在生命体征监测场景，边缘节点通过 AI 模型实时分析患者心率、血压等数据，判断患者健康状态，若出现异常立即生成预警决策；在医学影像处理场景，边缘节点通过轻量化影像分割模型，实时提取病灶特征，生成初步诊断建议。在云端协同分析环节，边缘节点将本地分析结果与关键原始数据上传至云端，云端部署复杂 AI 模型，对多边缘节点上传的数据进行全局汇总分析与深度挖掘，优化边缘节点 AI 模型参数，提升本地分析精度；同时，云端将全局分析结果反馈至边缘节点，为边缘节点的本地决策提供支撑。通过分布式分析，边缘计算实现了医疗数据的实时处理与智能决策，兼顾了决策的及时性与精准性。^①

二、边缘计算支撑的低延迟医疗服务实现路径

（一）低延迟远程医疗服务实现

边缘计算结合 5G 技术，实现低延迟远程医疗服务，推动优质医疗资源下沉。在远程会诊场景，基层医院部署边缘节点，连接远程会诊终端、医学影像设备等，基层医生将患者诊疗数据、影像数据上传至本地边缘节点，边缘节点对数据进行实时预处理与压缩，通过 5G 网络传输至上级医院边缘节点；上级医院医生通过终端实时接收数据，与基层医生进行高清视频会诊，会诊意见经边缘节点实时反馈至基层医院，实现远程诊疗的实时协同。在远程手术指导场景，上级医院专家通过边缘节点连接的手术指导终端，实时接收基层医院手术现场的高清视频与手术设备运行数据，通过低延迟网络向基层手术医生下达指导指令，确保手术指导的及时性与准确性。某区域远程医疗平台的实践显示，应用边缘计算后，远程会诊数据传输延迟降低至 50ms 以内，视频画面无卡顿，远程手术指导响应时间缩短 60%，有效提升了远程医疗服务质量。

（二）低延迟医疗设备协同服务实现

边缘计算实现医院内各类医疗设备的低延迟协同，提升医疗设备的运行效率与诊疗协同能力。在手术机器人协同场景，手术室边缘节点连接手术机器人、导航设备、生命体征监测设备等，各设备数据通过边缘节点实时交互，手术机器人根据导航数据与患者生命体征数据实时调整手术动作，确保手术精准性与安全

① 赵治远, 樊利军. 基于边缘计算的医院实时数据采集与处理系统设计 [J]. 信息与电脑, 2025, 37 (14): 87-89.

性；在影像设备协同场景，影像科边缘节点连接 CT、MRI、超声等设备，实现设备间数据的实时共享与协同工作，例如患者完成 CT 检查后，影像数据实时传输至超声设备，为超声检查提供参考，提升检查效率。同时，边缘节点实时监测医疗设备运行状态数据，通过 AI 算法预测设备故障风险，提前触发维护预警，减少设备故障停机时间。某医院的实践显示，应用边缘计算后，医疗设备协同响应时间缩短 70%，设备故障预警准确率提升 85%，设备利用率提升 25%。

边缘计算为应急医疗服务提供低延迟、高可靠的技术支撑，提升突发公共卫生事件与紧急医疗救援的处置效率。在突发公共卫生事件（如疫情）场景，医院在发热门诊、核酸检测点等关键区域部署边缘节点，实时采集就诊患者数据、核酸检测数据，边缘节点对数据进行实时分析与统计，快速上报至疫情防控指挥中心，为疫情防控决策提供实时数据支撑；同时，边缘节点支持多区域数据的实时协同，实现疫情数据的全局监控与快速响应。在紧急医疗救援场景，急救车移动边缘节点实时采集患者生命体征数据，通过 5G 网络快速传输至医院急诊边缘节点，医院提前做好救治准备；救援现场边缘节点与医院急诊边缘节点、消防、公安等部门边缘节点实现数据协同，快速调配救援资源，提升救援效率。某城市应急医疗体系的实践显示，应用边缘计算后，突发公共卫生事件数据上报延迟缩短 80%，紧急医疗救援响应时间缩短 25%，救援成功率提升 18%。

三、应用效果与面临的挑战

（一）典型应用效果

国内多家三甲医院与区域医疗中心的边缘计算应用实践显示，边缘计算在医院信息化管理中的应用取得了显著成效。在实时性提升方面，医疗数据处理延迟从传统的秒级缩短至毫秒级，平均延迟降低 75% 以上；临床诊疗、应急救援等场景的服务响应时间平均缩短 40%-60%，为患者救治争取了宝贵时间。在效率提升方面，医院临床诊疗效率提升 30%-40%，门诊患者平均就诊时间缩短 30% 以上，医疗设备利用率提升 25%-35%；跨科室、跨区域医疗协同效率提升 50% 以上，推动了优质医疗资源的下沉与共享。在安全可靠方面，医疗数据本地处理减少了数据传输风险，数据安全事件发生率降低 60% 以上；多边缘节点冗余部署与本地自治能力，使医疗服务连续性保障率提升至 99.9% 以上，有效降低了网络中断、设备故障等带来的医疗风险。

（二）核心挑战

边缘计算通过本地实时数据处理与服务响应，实现低延迟临床诊疗服务。在门诊诊疗场景，患者通过门诊边缘节点连接的自助终端完成挂号、缴费、预约检查等操作，边缘节点实时处理相关请求并反馈结果，减少患者排队等待时间；医生通过移动医护终端调取患者历史诊疗数据（由边缘节点本地缓存），结合实时采集的患者症状数据，快速做出诊断并开具处方，处方数据经边缘节点实时同步至药房，实现“诊疗-取药”流程的高效衔接。在住院诊疗场景，边缘节点实时监测患者生命体征数据，若出现异常立即预警并推送至医护人员终端，医护人员可快速响应并采取医疗干预措施；同时，边缘节点支持医护人员实时调取患者检查报告、影像数据等，提升查房、会诊效率。某三甲医院的实践显示，应用边缘计算后，门诊患者平均就诊时间缩短 30%，住院患者异常情况响应时间缩短至 2 分钟以内，临床诊疗效率显著提升。

技术层面，边缘计算节点的算力资源有限，难以支撑复杂医疗 AI 模型的实时运行；不同厂商的边缘设备与软件平台兼容性不足，存在“设备孤岛”“平台孤岛”问题，影响多节点协同；边缘节点与云端、终端设备间的网络连接稳定性受环境影响较大，在复杂医院环境（如地下楼层、偏远区域）可能出现网络中断或延迟波动；边缘计算架构的算力调度算法尚不完善，难以实现全局算力资源的最优配置。管理层面，缺乏统一的边缘计算在医院信息化应用的标准与规范，各医院的应用模式、技术选型差异较大，不利于行业推广；边缘节点的部署、运维需要专业技术团队，中小医院的技术实力与资金投入不足，难以支撑边缘计算的规模化应用；医疗数据的分布式存储与共享带来了数据管理难度的提升，数据主权、责任划分不明确。合规层面，边缘计算节点的本地数据存储与处理可能涉及患者隐私数据的本地化管理，如何确保符合医疗数据安全合规要求（如《数据安全法》《个人信息保护法》）是重要挑战；边缘计算的分布式架构使数据审计难度增加，难以实现数据全生命周期的合规追溯。

（三）优化方向

技术优化方面，研发高性能边缘计算节点设备，提升边缘节点的算力与存储能力；推动边缘计算设备与软件平台的标准化，制定统一的接口规范与通信协议，提升设备与平台的兼容性；优化“云-边-端”协同网络架构，采用 5G、WiFi 6 等高速网络技术，提升网络连接稳定性；研发智能算力调度算法，结合医疗业务

需求动态分配边缘节点与云端的算力资源，实现全局算力优化配置。管理优化方面，制定边缘计算在医院信息化应用的行业标准与规范，统一应用模式与技术选型；加强医院技术人员的边缘计算相关培训，提升边缘节点部署、运维能力；建立跨医院、跨区域的边缘计算协同管理机制，实现算力资源与医疗数据的共享协同；降低边缘计算部署成本，推出适合中小医院的轻量化边缘计算解决方案。合规优化方面，建立边缘计算环境下的医疗数据安全管理体系，采用数据加密、访问控制、数据脱敏等技术，保障患者隐私数据安全；制定边缘计算数据审计规范，实现数据全生命周期的合规追溯；加强边缘计算应用的合规评估，确保符合相关法律法规要求。

第三节 边缘计算赋能的移动医疗设备本地算力增强

一、移动医疗设备应用现状与算力瓶颈

（一）移动医疗设备应用场景与核心价值

移动医疗设备作为医院信息化管理的关键终端载体，已广泛应用于临床诊疗、急诊急救、慢病管理、院感防控等核心场景。在临床诊疗场景，移动护理终端、移动医生工作站可实现床旁患者信息核对、生命体征采集、电子医嘱执行、诊疗记录实时录入等功能，打破了诊疗行为对固定诊室的依赖；在急诊急救场景，车载移动监护设备、便携式超声仪、移动心电图机等可实现院前患者生命体征实时监测与初步诊断，为院内救治争取时间；在慢病管理场景，智能手环、便携式血糖仪、血压计等可实现患者居家康复数据的持续采集与远程传输，支撑慢病精细化管理；在院感防控场景，移动体温监测仪、智能消毒设备可实现全院区人员体温筛查与环境消毒轨迹追溯，提升院感防控效率。移动医疗设备的普及，有效提升了医疗服务的灵活性、及时性与覆盖面，是推动医院信息化向“全流程、全场景”延伸的核心支撑。

（二）移动医疗设备核心算力瓶颈分析

尽管移动医疗设备应用广泛，但受限于体积、功耗、成本等因素，其本地算力普遍存在显著瓶颈，难以支撑复杂医疗数据的实时处理需求，主要体现在三个方面：一是实时数据处理能力不足，移动医疗设备采集的医学影像、生命体征流数据、高清视频等数据量庞大且时效性强，如便携式超声仪产生的超声影像数据、

移动监护设备的多参数生命体征数据,需快速完成降噪、增强、特征提取等处理,但设备本地 CPU、GPU 算力有限,难以实现毫秒级处理;二是复杂 AI 算法部署困难,基于深度学习的辅助诊断算法(如影像病灶识别、生命体征异常预警)对算力需求较高,移动医疗设备难以承载此类算法的本地运行,只能将数据上传至云端处理,导致响应延迟增加;三是离线运行能力薄弱,在网络信号差或中断场景(如偏远地区急救、医院地下楼层),移动医疗设备无法依赖云端算力,本地算力不足会导致数据处理中断,影响医疗服务连续性;同时,数据远程传输过程中还面临带宽占用高、隐私泄露风险大等问题。

二、边缘计算赋能移动医疗设备算力增强的技术路径

(一) 边缘节点就近算力卸载与协同计算

采用“设备本地轻计算+边缘节点重计算”的算力卸载模式,实现移动医疗设备算力的精准增强。通过在医院各楼层、门诊楼、住院楼、急救中心等移动医疗设备高频使用区域部署边缘节点,构建覆盖全院的边缘算力网络;移动医疗设备通过 5G、WiFi 6 等高速无线通信技术与就近边缘节点建立连接,将复杂数据处理任务(如医学影像预处理、AI 辅助诊断、大数据统计分析)卸载至边缘节点,设备本地仅承担数据采集、简单预处理(如数据格式化)与结果展示等轻量任务。边缘节点配备高性能 CPU、GPU 与专用计算芯片,可同时承接多台移动设备的算力卸载需求,通过任务调度算法实现算力资源的动态分配;同时,边缘节点与移动设备之间采用低延迟通信协议,确保数据传输与处理的实时性。例如,便携式超声仪将采集的超声影像数据卸载至门诊楼边缘节点,边缘节点通过轻量化 AI 算法快速完成病灶识别与标记,处理结果实时反馈至设备终端,医生可现场查看诊断建议,无需等待云端处理。

(二) 轻量化 AI 模型部署与边缘适配优化

针对移动医疗设备算力有限的特点,通过 AI 模型轻量化改造与边缘适配优化,实现复杂诊断算法的就近部署与高效运行。采用模型剪枝、量化、蒸馏等轻量化技术,在保证诊断精度的前提下,降低 AI 模型的参数量与计算量,使其可适配边缘节点的算力需求;同时,根据不同移动医疗设备的应用场景,定制化开发轻量化 AI 模型,如针对移动监护设备的生命体征异常预警模型、针对便携式影像设备的病灶快速识别模型。边缘节点部署统一的 AI 模型管理平台,实现模

型的统一更新、部署与运维；移动医疗设备通过边缘节点调用轻量化 AI 模型，无需本地存储复杂模型，进一步降低设备算力消耗。此外，通过边缘节点与云端的模型协同训练，将云端训练的高精度模型轻量化后下发至边缘节点，提升边缘侧 AI 诊断的准确性；边缘节点将本地处理数据反馈至云端，用于模型迭代优化，形成“云 - 边 - 端”协同的模型进化体系。

（三）边缘缓存与离线算力保障机制

构建边缘缓存与离线算力保障机制，解决移动医疗设备在网络中断场景下的算力不足问题。边缘节点配备大容量本地存储设备，缓存常用的医疗数据（如患者历史诊疗记录、标准医学影像模板）、轻量化 AI 模型、诊疗规范等资源；当移动医疗设备处于离线状态时，可直接调用边缘节点缓存的资源开展本地数据处理，保障医疗服务不中断。例如，急救车配备移动边缘节点，缓存急救相关的 AI 诊断模型与常见病症诊疗方案，在偏远地区网络中断时，可独立完成患者生命体征数据处理与初步诊断，网络恢复后再将数据同步至医院云端。同时，边缘节点采用本地数据加密存储与访问控制技术，保障缓存数据的安全性与隐私性；通过缓存更新策略，定期同步云端最新数据与模型，确保离线状态下的诊疗服务质量。

（四）算力网络动态调度与负载均衡

依托算力网络技术，实现边缘算力资源的全局调度与负载均衡，提升移动医疗设备算力增强的稳定性与高效性。构建全院级边缘算力网络调度平台，实时监控各边缘节点的算力资源占用情况（CPU、GPU 利用率）、任务处理队列、网络状态等信息；当某一区域边缘节点算力负载过高时，调度平台自动将部分移动医疗设备的算力卸载任务分配至邻近空闲边缘节点；当边缘节点出现故障时，快速切换至冗余边缘节点，保障算力服务的连续性。同时，调度平台根据移动医疗设备的业务优先级（如急诊急救设备优先级高于普通门诊设备）分配算力资源，确保关键医疗场景的算力需求得到优先满足。通过算力网络的动态调度，实现全院边缘算力资源的优化配置，避免局部算力过载或闲置，提升整体算力利用效率。

三、典型应用场景与实施效果

（一）移动护理终端算力增强场景

某三甲医院在住院楼各楼层部署边缘节点，为移动护理终端提供算力增强服

务。移动护理终端采集患者生命体征数据（心率、血压、血氧等）后，将数据处理与异常预警任务卸载至就近边缘节点；边缘节点通过轻量化 AI 模型实时分析数据，若发现异常立即推送预警信息至护理终端与护士站，同时关联患者历史诊疗数据，提供初步干预建议。实施后，移动护理终端数据处理延迟从原来的 2-3 秒缩短至 300 毫秒以内，生命体征异常预警响应时间缩短 75%；护士非护理事务处理时间减少 40%，护理工作效率显著提升；患者住院期间不良事件发生率降低 35%，护理质量得到有效保障。

（二）院前急救移动设备算力增强场景

某急救中心为急救车配备移动边缘节点，搭载轻量化超声影像诊断、心电图分析等 AI 模型，为车载移动医疗设备提供算力支撑。急救过程中，便携式超声仪、心电图机采集的患者数据实时卸载至移动边缘节点，节点快速完成数据处理与诊断分析，生成初步诊断报告并实时传输至医院急诊科室；同时，在网络中断场景下，移动边缘节点可独立完成数据处理，保障急救诊疗不中断。实施后，院前急救数据处理时间缩短 80%，初步诊断准确率提升 45%；院内急诊科室可提前获取患者诊疗数据，做好救治准备，患者到院后救治响应时间缩短 60%，危重患者救治成功率提升 18%。

（三）慢病管理移动监测设备算力增强场景

某医院在社区卫生服务中心部署边缘节点，为慢病患者的智能穿戴设备、便携式监测设备提供算力增强服务。患者居家监测的血糖、血压、心率等数据通过 5G 网络传输至社区边缘节点，节点通过 AI 模型实时分析数据，识别慢病恶化风险，若发现异常立即推送预警信息至患者与家庭医生终端；同时，边缘节点缓存患者慢病管理方案，为家庭医生提供诊疗参考。实施后，慢病患者数据监测延迟缩短至 500 毫秒以内，风险预警准确率提升 50%；家庭医生随访效率提升 40%，慢病患者并发症发生率降低 30%，有效减轻了医院诊疗压力。

第四节 边缘与云协同算力网络在医院多院区一体化业务中的应用模式

一、医院多院区一体化业务发展需求与算力支撑痛点

（一）多院区一体化业务核心发展需求

随着医疗行业规模化发展，多院区布局已成为大型医院扩大服务范围、优化资源配置的重要模式，多院区一体化业务发展核心需求体现在四个方面：一是诊疗服务同质化，要求各院区遵循统一的诊疗规范、质量标准，实现患者在任意院区都能享受同等质量的医疗服务；二是资源共享高效化，需实现各院区医疗设备、医护人员、药品、数据等资源的跨院区共享与优化调度，提升资源利用效率；三是业务流程协同化，要求打通各院区挂号、诊疗、检查、转诊、结算等业务流程，实现跨院区业务的无缝衔接；四是管理决策精准化，需整合各院区业务数据，进行全局分析与监控，为医院管理决策提供数据支撑。一体化业务的开展，对算力资源的分布式部署、实时协同、动态调度提出了更高要求。

（二）多院区一体化业务算力支撑痛点

传统算力支撑模式（单一云端算力或各院区独立算力）难以满足多院区一体化业务需求，存在三大核心痛点：一是跨院区数据处理延迟高，传统云端算力模式下，各院区业务数据需传输至远端云端处理，跨院区数据传输距离远、延迟高，尤其是高清医学影像、实时诊疗视频等大流量数据，易出现传输卡顿，影响跨院区协同诊疗效率；二是算力资源配置不均衡，各院区独立部署算力资源，导致部分院区算力紧张、部分院区算力闲置，无法实现全局算力优化配置；同时，大型医疗设备（如手术机器人、高端影像设备）配套的算力资源难以跨院区共享，资源浪费严重；三是业务连续性保障不足，单一云端或单院区算力节点故障时，会导致相关业务中断；在网络中断场景下，各院区无法依赖远端算力，本地业务处理能力受限，影响一体化服务连续性；此外，数据集中传输至云端还面临带宽占用高、隐私泄露风险大等问题。

二、边缘与云协同算力网络的核心架构设计

（一）架构核心理念

边缘与云协同算力网络以“云端统筹、边缘协同、全域互联、动态调度”为核心设计理念，构建“云-边-端”三级算力协同架构，实现算力资源的分布式部署与全局优化配置。云端负责全局算力资源调度、大数据分析、模型训练、业务管理等重计算与管控任务；边缘节点部署在各院区及核心业务区域，负责本地业务数据的实时处理、就近服务、数据缓存等轻计算与实时响应任务；终端设备（医疗设备、医护终端、患者终端）负责数据采集与业务交互，根据需求调用边缘或云端算力资源。通过算力网络技术实现云端与边缘、边缘与边缘之间的算力协同与数据共享，形成“全局管控+本地响应”的算力服务模式，精准匹配多院区一体化业务的算力需求。

（二）三级算力协同架构详细组成

云端算力层：部署在医院总院核心数据中心，由高性能服务器集群、云计算平台、数据中台、AI训练平台组成。核心功能包括：全局算力资源调度，通过算力网络调度系统实时监控各边缘节点算力状态，动态分配算力资源；大数据分析 & 挖掘，整合各院区业务数据，开展全局业务分析、质量监控、决策支持等；AI模型训练与优化，基于海量医疗数据训练高精度AI模型，轻量化后下发至边缘节点；业务管理与运维，实现多院区一体化业务的统一管理、权限控制、安全审计等。云端算力层具备海量存储与大规模并行计算能力，为多院区一体化业务提供全局算力支撑。

边缘算力层：在各分院区、门诊楼、住院楼、急救中心等核心区域部署边缘节点，形成分布式边缘算力集群。每个边缘节点配备高性能计算设备、本地存储设备、网络转发设备，具备独立的计算、存储、网络能力。核心功能包括：本地业务实时处理，承接各院区门诊诊疗、检查检验、护理服务等本地业务的数据处理任务，实现低延迟响应；算力卸载与协同，承接终端设备的算力卸载任务，与云端协同完成复杂业务处理；数据缓存与同步，缓存常用医疗数据、AI模型、诊疗规范等资源，保障离线业务开展，同时定期与云端同步数据；跨院区边缘协同，通过算力网络实现各边缘节点之间的算力共享与任务协同，支撑跨院区业务开展。

终端接入层：涵盖各院区医疗设备（影像设备、手术机器人、监护设备）、医护终端（移动医生工作站、护理终端）、患者终端（自助服务终端、手机APP）、物联网传感器等。终端设备通过5G、WiFi 6、光纤等通信技术与边缘节点或云端建立连接，根据业务需求灵活调用算力资源；同时，终端设备实时采集业务数据，传输至边缘或云端进行处理，实现业务数据的全流程流转。

算力调度与网络层：作为架构核心枢纽，由算力调度平台、SDN（软件定义网络）控制器、安全网关组成。算力调度平台基于业务类型、优先级、算力需求、网络状态等因素，智能分配算力资源，实现“云-边-端”算力协同；SDN控制器实现网络资源的动态调度与优化，保障数据传输的高速性与稳定性；安全网关采用数据加密、访问控制、入侵检测等技术，保障算力网络与数据传输的安全性。

三、边缘与云协同算力网络在多院区一体化业务中的典型应用模式

（一）跨院区协同诊疗与远程医疗应用模式

依托边缘与云协同算力网络，构建跨院区协同诊疗与远程医疗平台，实现优质医疗资源的跨院区共享。在远程会诊场景，分院区医生通过终端发起会诊请求，将患者电子病历、医学影像等数据上传至本地边缘节点；边缘节点对数据进行预处理（如影像降噪、格式转换）后，通过算力网络同步至总院边缘节点与云端；总院专家通过终端实时调用边缘节点处理后的高清影像数据与云端存储的患者历史数据，开展高清视频会诊，会诊意见实时反馈至分院区边缘节点，指导本地诊疗。在远程手术指导场景，手术现场边缘节点实时采集手术视频、手术机器人运行数据，通过5G+算力网络高速传输至远端指导专家终端；云端算力平台对手术数据进行实时分析，为专家提供辅助决策支持；专家的指导指令通过边缘节点实时下发至手术机器人，实现低延迟远程手术指导。协同算力网络的应用，将跨院区远程会诊延迟缩短至50毫秒以内，手术指导响应延迟缩短至10毫秒以内，大幅提升了跨院区诊疗效率与质量。

（二）跨院区医疗资源协同调度应用模式

基于边缘与云协同算力网络，构建跨院区医疗资源协同调度平台，实现算力、设备、人员等资源的全局优化配置。在算力资源调度方面，云端算力调度平台实时监控各院区边缘节点的算力负载，当某院区边缘节点算力不足时，自动调度其他院区空闲边缘节点或云端算力进行补充；例如，某分院区开展大型体检时，影

像数据处理需求激增,云端调度平台将部分影像处理任务分配至总院边缘节点与空闲分院区边缘节点,实现算力负载均衡。在医疗设备调度方面,平台实时监控各院区大型医疗设备的运行状态、使用情况与算力需求,患者可跨院区预约空闲设备检查,检查数据通过边缘节点实时共享至就诊院区;同时,设备配套的算力资源通过算力网络实现跨院区共享,提升设备利用率。在医护人员调度方面,平台基于各院区业务量、医护人员技能、算力支撑能力等因素,动态调配医护人员跨院区支援,同时通过边缘节点为支援人员提供本地业务数据与算力支撑,确保工作高效开展。实施后,医院整体算力资源利用率提升 40% 以上,大型医疗设备利用率提升 35% 以上,跨院区资源调度响应时间缩短 60% 以上。

(三) 跨院区一体化业务流程协同应用模式

借助边缘与云协同算力网络,打通各院区业务系统,实现挂号、诊疗、检查、转诊、结算等一体化业务流程的无缝协同。在跨院区挂号与结算场景,患者通过任意院区终端或线上渠道挂号,挂号数据实时传输至本地边缘节点,边缘节点同步至云端数据中台完成身份认证与信息录入;结算时,边缘节点实时调取患者跨院区诊疗费用数据,通过云端算力平台完成医保报销核算与费用结算,结算结果实时反馈至患者终端,实现“一次挂号、全域就诊、一键结算”。在跨院转诊场景,转诊申请数据通过转出院区边缘节点上传至云端,云端调度平台同步至转入院区边缘节点,转入院区医生可通过边缘节点实时调取患者转出院区诊疗数据,提前制定诊疗方案;患者转至后,边缘节点实现转诊数据与本地诊疗数据的无缝对接,避免重复检查。协同算力网络的应用,使跨院区挂号结算时间缩短至 30 秒以内,转诊流程时间缩短 70% 以上,患者跨院区就医体验显著提升。

第八章 新一代通信技术在医院管理流程优化中的应用

第一节 基于“通信+”的全闭环就诊流程再造

一、传统就诊流程痛点与“通信+”再造核心逻辑

（一）传统就诊流程核心痛点

传统医院就诊流程涵盖挂号、候诊、诊疗、检查、缴费、取药/取报告等多个环节，存在流程繁琐、信息不对称、等待时间长、各环节衔接不畅等核心痛点。从患者视角来看，挂号需现场排队或依赖单一线上渠道，易出现号源紧张或操作不便问题；候诊阶段缺乏精准时间预判，患者长时间无效等待，就医体验差；检查与诊疗环节脱节，检查申请、结果反馈需人工传递，易出现数据丢失或延迟，导致诊疗效率低下；缴费环节需在不同窗口多次排队，支付方式单一；取药、取报告环节同样存在排队等待问题，且无法实时获取进度通知。从医院管理视角来看，各环节数据分散在独立系统，缺乏实时联动，难以实现流程全局管控；医护人员需花费大量时间处理非诊疗类事务（如信息核对、单据传递），核心诊疗效率被稀释；流程瓶颈难以精准定位，优化决策缺乏数据支撑。

（二）“通信+”全闭环就诊流程再造核心逻辑

基于5G、物联网、大数据、云计算等新一代通信技术，构建“通信+”全闭环就诊流程再造核心逻辑，以“患者为中心”，实现就诊全流程的数字化、智能化、协同化升级。核心逻辑体现在三个维度：一是数据实时联动，通过通信技术打通挂号、候诊、诊疗、检查、缴费、取药等各环节信息系统，实现患者数据、诊疗数据、设备数据的实时采集、传输与共享；二是服务精准触达，依托移动通信技术（如5G、4G、短信、小程序推送），为患者提供全流程精准信息推送（如挂号成功通知、候诊提醒、检查预约时间、缴费提醒、报告推送），减少信息不对称；三是流程协同优化，通过通信技术实现医护、医技、行政、后勤等多岗位

的实时协同，简化不必要环节，实现各流程节点的无缝衔接；同时，基于通信技术采集的全流程数据，进行流程瓶颈分析与优化，提升管理精准度。

二、“通信+”全闭环就诊流程关键环节再造实践

（一）院前智能预约与精准引导环节

依托新一代通信技术构建多元化、智能化院前预约体系，实现预约精准化与引导个性化。在预约渠道方面，整合 5G 消息、微信小程序、APP、电话、第三方平台等多种通信渠道，打造全渠道预约入口，患者可根据自身习惯选择预约方式；通过 5G 技术的高带宽、低延迟特性，实现预约界面的快速加载与操作响应，提升预约体验。在预约服务方面，引入 AI 智能分诊功能，患者通过语音或文字描述症状后，系统基于大数据分析自动匹配对应科室与医生，推荐合适的就诊时间，避免挂错号、跑错科问题；同时，支持分时段精准预约，将就诊时间精准到 30 分钟内，减少患者候诊等待时间。在院前引导方面，预约成功后，系统通过 5G 消息或短信向患者推送就诊指南，包含医院地理位置、交通路线、停车场信息、就诊流程说明等；患者到达医院周边后，可通过手机小程序获取院内导航服务，基于物联网定位技术引导患者精准找到就诊科室、检查室、缴费窗口等位置，解决院内“找路难”问题。

（二）院中协同诊疗与高效流转环节

通过“通信+”技术实现院中各诊疗环节的协同联动，提升诊疗效率与流转顺畅度。在候诊环节，基于 5G+ 物联网技术实现患者精准候诊管理，患者进入医院后通过扫码签到，系统自动更新候诊队列，实时向患者推送候诊进度（如前方等待人数、预计就诊时间），患者可在院内自由活动，无需在诊室门口排队等候；同时，系统向医生推送患者基本信息、既往病史、预约症状等数据，便于医生提前了解病情，提升诊疗准备效率。在诊疗环节，采用 5G+ 移动医护终端实现诊疗数据的实时采集与共享，医生通过移动终端实时调取患者电子病历、检查报告、影像数据等，无需纸质单据传递；诊疗过程中，医生可直接通过终端开具电子检查申请、电子处方，申请与处方数据实时同步至检查科室、药房，实现“诊疗-检查-取药”的无缝衔接。在检查环节，依托 5G+ 医学影像传输技术，实现影像数据的高速、高清传输，检查设备完成检查后，影像数据实时推送至医生诊断终端与 PACS 系统，医生可快速阅片并出具诊断报告，报告完成后实时推送至

患者终端，避免患者二次往返取报告。

（三）院后便捷结算与随访管理环节

借助新一代通信技术优化院后结算与随访管理流程，提升患者出院体验与康复管理质量。在结算环节，构建多元化、无接触式结算体系，患者可通过手机小程序、APP、自助终端等渠道，基于 5G 技术实现实时在线缴费，支持医保电子凭证直接支付、微信、支付宝、银行卡等多种支付方式；缴费完成后，系统实时生成电子发票并推送至患者手机，无需现场打印；对于住院患者，出院前系统自动核算费用明细，通过 5G 消息向患者推送费用清单，患者在线确认后即可完成结算，大幅缩短出院办理时间。在随访管理环节，基于 5G+ 物联网 + 大数据技术构建智能化随访体系，出院患者通过智能穿戴设备（如血压计、血糖仪、心率监测手环）实时采集康复期间的生命体征数据，数据通过 5G 网络实时传输至医院随访管理系统；系统通过 AI 算法分析数据，若发现异常立即推送至医护人员终端，医护人员及时开展远程干预；同时，系统根据患者病情制定个性化随访计划，通过短信、电话、视频等通信方式定期开展随访，推送康复指导、用药提醒等信息，提升患者康复效果。

三、核心支撑技术与应用效果

（一）核心支撑技术

支撑“通信+”全闭环就诊流程再造的核心技术包括 5G 技术、物联网技术、大数据与 AI 技术、云计算技术等。5G 技术凭借高带宽、低延迟、广连接特性，实现医疗数据（如高清医学影像、实时生命体征数据）的高速传输与实时交互，为远程诊疗、移动医护等场景提供网络支撑；物联网技术通过部署各类传感器、智能终端，实现患者、医疗设备、环境等多维度数据的实时采集，为流程优化提供数据基础；大数据与 AI 技术用于患者需求分析、智能分诊、流程瓶颈识别、康复数据监测等，提升流程的智能化水平；云计算技术为全流程数据提供稳定、高效的存储与计算支撑，实现数据的集中管理与共享协同。

（二）典型应用效果

国内多家三甲医院的“通信+”就诊流程再造实践取得了显著成效。在效率提升方面，患者平均就诊时间从传统的 2-3 小时缩短至 1 小时以内，门诊患者候诊时间平均缩短 60% 以上，检查报告出具时间从平均 2-3 天缩短至几小时内，

出院办理时间从平均 1-2 小时缩短至 30 分钟以内；医护人员非诊疗事务处理时间减少 40% 以上，核心诊疗效率显著提升。在体验优化方面，患者满意度从传统的 75% 左右提升至 95% 以上，线上预约率提升至 85% 以上，无接触式结算占比超过 90%，有效减少了患者排队等待与人员聚集。在管理提升方面，医院实现了就诊全流程数据的实时监控与分析，流程瓶颈定位精准度提升 80% 以上，管理决策的科学性与时效性显著增强；医疗资源利用率提升 30% 以上，有效缓解了医疗资源紧张问题。

第二节 通信技术支撑的多院区业务协同与信息互通

一、多院区管理现状与业务协同核心痛点

（一）多院区管理现状

随着医疗行业的发展，大型医院多院区布局成为趋势，通过建设分院区、医联体等形式，实现医疗资源的优化配置与下沉。当前多院区管理模式主要分为紧密型、半紧密型与松散型三类，紧密型多院区实行“人、财、物、信息、管理”一体化管理，半紧密型与松散型多院区则在保持一定独立性的基础上，开展业务协同与资源共享。无论何种管理模式，多院区都面临着地理空间分散、业务类型多样、患者流动频繁、资源调配复杂等共性问题，对业务协同与信息互通提出了更高要求。尤其是在分级诊疗政策推动下，多院区需实现从门诊、住院、检查、手术到康复的全流程协同，确保医疗服务的连续性与一致性。

（二）多院区业务协同与信息互通核心痛点

当前多院区业务协同与信息互通主要面临四大核心痛点：一是信息孤岛问题突出，各院区往往拥有独立的信息系统（如 HIS、LIS、PACS、电子病历系统），系统架构、数据格式、接口标准不统一，导致患者数据、诊疗数据、资源数据无法跨院区共享，患者在不同院区就诊时需重复检查、重复建档，医疗资源浪费严重；二是业务协同效率低下，由于信息不畅通，多院区之间的转诊、会诊、检查预约等业务需通过人工传递单据、电话沟通等传统方式开展，流程繁琐、周期长，影响患者救治效率；三是资源调配不均衡，各院区的医疗设备、医护人员、床位等资源信息无法实时共享，导致部分院区资源紧张、部分院区资源闲置，资源利

用效率低下；四是质量管控难度大，多院区医疗服务标准、诊疗规范难以统一，医疗质量监测数据无法实时汇总分析，难以实现全院区医疗质量的统一管控，存在医疗安全风险。

二、通信技术支撑的多院区信息互通体系构建

（一）信息互通体系架构设计

基于新一代通信技术构建“云端协同+边缘接入+全域互联”的多院区信息互通体系，架构从上至下分为云端数据中心层、通信传输层、边缘接入层与终端应用层。云端数据中心层部署在总院核心机房，构建统一的医疗数据中台与业务中台，实现多院区数据的集中存储、管理与共享；数据中台整合各院区患者数据、诊疗数据、资源数据等，通过数据标准化处理（如采用HL7 FHIR、DICOM等标准），实现数据格式统一；业务中台整合各院区核心业务系统功能，为多院区协同业务提供标准化服务支撑。通信传输层采用5G+光纤双链路冗余架构，5G网络实现灵活、快速的无线接入，光纤网络提供高速、稳定的有线传输，保障跨院区数据传输的高速性、低延迟与可靠性；同时，部署VPN、防火墙等安全技术，保障数据传输安全。边缘接入层部署在各分院区，通过边缘节点实现分院区本地信息系统与云端数据中心的对接，负责本地数据的预处理、缓存与上传，提升数据访问效率；在网络中断时，边缘节点可保障本地核心业务的正常运行。终端应用层涵盖各院区医护终端、患者终端、医疗设备终端等，通过标准化接口接入信息互通体系，实现数据的实时交互与业务的协同开展。

（二）核心信息互通功能实现

多院区信息互通体系核心实现三大功能：一是患者数据全域共享，通过统一的患者主索引（EMPI）技术，为患者建立唯一的身份标识，实现各院区患者电子病历、检查报告、化验结果、用药记录、住院记录等数据的实时共享，患者在任意院区就诊时，医护人员可快速调取完整诊疗数据，避免重复检查；二是业务数据实时同步，各院区HIS、LIS、PACS等系统数据实时同步至云端数据中心，实现挂号、缴费、预约、诊疗等业务数据的跨院区互通，支持患者跨院区挂号、跨院区缴费、跨院区预约检查等功能；三是资源信息动态共享，各院区医疗设备、医护人员、床位、药品等资源信息实时上传至云端，构建全域资源动态管理平台，实现资源信息的实时查询与可视化监控。

三、通信技术驱动的多院区业务协同场景实践

（一）跨院区分级诊疗与转诊协同

依托 5G+ 云端协同通信技术,构建跨院区分级诊疗与转诊协同体系,实现“基层首诊、双向转诊、急慢分治、上下联动”。在向下转诊场景,总院医生通过信息互通体系将康复期患者的诊疗数据、康复计划实时推送至分院区或社区医院,同时通过 5G 视频会诊向基层医生提供康复指导;基层医生可实时调取患者总院诊疗数据,精准开展康复治疗,患者无需往返总院,提升康复便利性。在向上转诊场景,基层医院医生发现疑难重症患者时,通过系统提交转诊申请,同时上传患者本地诊疗数据;总院医生实时接收转诊申请与患者数据,提前进行病情评估,确定接收科室与诊疗方案;患者转至总院后,无需重复检查,直接进入针对性诊疗流程,大幅缩短救治时间。某医疗集团的实践显示,应用该协同体系后,跨院区转诊流程时间缩短 70% 以上,疑难重症患者救治效率提升 40% 以上,基层医院康复诊疗能力提升 50% 以上。

（二）跨院区远程会诊与多学科协作（MDT）

基于 5G+ 高清视频 + 实时数据共享技术,构建跨院区远程会诊与多学科协作（MDT）平台,打破地理空间限制,实现优质医疗资源的跨院区共享。在远程会诊场景,分院区医生通过平台发起会诊请求,实时上传患者电子病历、医学影像、化验结果等数据;总院专家通过高清视频与分院区医生、患者进行实时交互,同步查看患者完整诊疗数据,出具会诊意见;同时,可通过 5G 技术远程操控分院区医疗设备,开展远程检查指导。在 MDT 场景,针对复杂疑难病例,由牵头科室通过平台发起多学科协作请求,邀请总院与各分院区相关科室专家参与会诊;专家通过平台实时共享病例数据,开展高清视频讨论,共同制定诊疗方案;诊疗方案实时同步至各参与院区,指导后续诊疗开展。该平台的应用,使各院区专家资源得到充分整合,疑难病例诊断准确率提升 35% 以上,患者无需跨院区奔波即可享受多学科专家诊疗服务,就医体验显著提升。

（三）跨院区医疗资源协同调度

通过通信技术构建跨院区医疗资源协同调度平台,实现医护人员、医疗设备、床位、药品等资源的动态优化配置。在医护人员调度方面,平台实时显示各院区医护人员的在岗状态、专业特长、工作量等信息,当某院区出现医护人员短缺(如

突发公共卫生事件、大型手术需求）时，管理人员通过平台快速调配其他院区空闲医护人员，同时通过 5G 消息向相关人员推送调度指令与患者数据，确保医护人员快速到岗开展工作。在医疗设备调度方面，平台实时监控各院区大型医疗设备（如 CT、MRI、手术机器人）的运行状态、使用情况、预约队列等信息，患者可通过平台跨院区预约空闲设备检查，检查数据实时共享至就诊院区，避免设备资源闲置与患者等待；当某院区设备故障时，可快速调度其他院区设备接收患者，保障诊疗连续性。在床位与药品调度方面，平台实时更新各院区床位占用情况、药品库存信息，实现床位的跨院区预留与调配、药品的跨院区调拨，提升资源利用效率。某多院区医院的实践显示，应用资源协同调度平台后，医疗设备利用率提升 30% 以上，床位周转效率提升 25% 以上，跨院区资源调度响应时间缩短 60% 以上。

（四）跨院区医疗质量统一管控

借助通信技术与大数据分析，构建跨院区医疗质量统一管控体系，实现全院区医疗质量的实时监测、评估与改进。通过信息互通体系实时采集各院区诊疗数据、护理数据、院感数据、不良事件数据等质量监测指标，传输至云端质量管控平台；平台通过 AI 算法对数据进行实时分析，对比各院区医疗质量标准，识别质量隐患与薄弱环节，实时向各院区质控部门推送预警信息；同时，平台生成全院区医疗质量分析报告，为管理部门制定质量改进措施提供数据支撑。此外，通过 5G 视频技术实现跨院区医疗质量现场督导，总院质控专家可远程查看分院区诊疗流程、操作规范执行情况，实时提出改进建议；各院区之间通过平台共享质量管控经验与最佳实践，推动全院区医疗质量同质化提升。应用该体系后，某医疗集团各院区医疗质量达标率提升至 98% 以上，不良事件发生率降低 45% 以上，医疗质量同质化水平显著提升。

第三节 基于新一代通信技术的医院后勤智慧能力改造

一、医院后勤管理现状与智慧改造核心需求

（一）医院后勤管理核心痛点

医院后勤管理涵盖设施设备运维、能源管理、物资供应链、环境管控、安全保卫、餐饮服务等多个领域，是保障医院正常运转的核心支撑。当前传统后勤管理模式普遍存在管理粗放、响应滞后、效率低下、资源浪费等痛点：一是设施设备运维被动化，电梯、中央空调、医用气体、配电系统等关键设备依赖人工巡检，难以实时监测运行状态，故障发现不及时，易引发停机事故，影响医疗服务连续性；二是能源管理精细化不足，水、电、气等能源消耗数据采集滞后，缺乏实时分析与优化调控手段，能源浪费严重，运营成本居高不下；三是物资管理效率低下，药品、耗材、办公用品等物资的采购、存储、领用、盘点等环节依赖人工记录，数据不准确、更新不及时，易出现物资短缺或积压，影响诊疗服务开展；四是环境与安全管控碎片化，病房、手术室、药房等关键区域的温湿度、洁净度等环境参数监测不精准，安防监控、消防预警等系统独立运行，缺乏协同联动，应急处置能力薄弱；五是管理决策缺乏数据支撑，各后勤业务数据分散在独立系统，无法实现全局整合与分析，管理决策依赖经验判断，精准度与科学性不足。

（二）新一代通信技术驱动的智慧改造核心需求

基于 5G、物联网、WiFi 6、工业互联网等新一代通信技术，医院后勤智慧改造核心需求体现在四个维度：一是实时感知与精准监测，通过泛在通信网络连接各类后勤终端与传感器，实现设施设备运行状态、能源消耗、物资库存、环境参数、安防状态等数据的实时采集与精准监测；二是协同联动与智能响应，打破各后勤系统信息壁垒，实现设备运维、能源管控、物资管理、安防应急等业务的协同联动，提升故障处置、应急响应的时效性与精准性；三是智能优化与高效管控，依托通信技术传输的海量数据，结合边缘计算与算力网络实现数据实时分析与智能决策，优化资源配置，降低运营成本，提升管理效率；四是全流程追溯与风险预警，实现后勤业务全流程数据的可追溯，通过实时数据分析识别潜在风险，提前发出预警，保障后勤服务的稳定性与安全性。

二、新一代通信技术在后勤智慧改造中的关键应用场景

（一）关键设施设备智慧运维场景

依托 5G+ 物联网 + 边缘计算技术，构建关键设施设备智慧运维体系，实现从“被动维修”向“主动预警、预测性维护”转型。在设备感知层，通过在电梯、中央空调、医用气体系统、配电设备、污水处理设备等关键设施上部署振动传感器、温度传感器、压力传感器、电流电压传感器等物联网终端，实时采集设备运行参数（如振动频率、温度、压力、能耗、运行时长）；终端通过 5G 或 WiFi 6 网络将数据实时传输至就近边缘节点。在边缘计算层，边缘节点对设备运行数据进行实时分析，通过故障诊断算法识别设备异常状态，若发现参数超标或潜在故障，立即通过算力网络推送预警信息至运维管理平台与运维人员终端，明确故障位置、类型与严重程度；同时，基于历史运行数据与实时数据，通过预测性维护算法推算设备剩余使用寿命，生成个性化维护计划，指导运维人员提前开展维护工作。在远程运维场景，对于复杂设备（如大型中央空调、医用气体系统），运维人员可通过 5G 高清视频远程查看设备运行状态，通过远程控制终端对设备进行参数调整与故障排查；设备厂商专家可通过 5G 网络远程协助解决疑难故障，提升运维效率。某三甲医院的实践显示，应用该体系后，关键设施设备故障预警准确率提升至 95% 以上，故障停机时间缩短 60%，运维成本降低 35%，设备平均使用寿命延长 15%。

（二）全链路能源智慧管控场景

基于 5G+ 物联网 + 算力网络构建全链路能源智慧管控体系，实现医院水、电、气、热等能源消耗的实时监测、智能分析与优化调控。在能源数据采集环节，通过在各楼层、各科室、关键设备部署智能电表、水表、燃气表等物联网采集终端，实时采集能源消耗数据；终端通过 5G 窄带物联网（NB-IoT）技术将数据传输至边缘节点，NB-IoT 技术具备低功耗、广连接、低成本特性，可满足海量终端的长期稳定运行需求。在能源分析与调控环节，边缘节点对能源消耗数据进行实时预处理与初步分析，识别异常消耗（如漏电、漏水、燃气泄漏）并实时预警；同时，将数据同步至云端算力平台，平台基于海量历史数据与实时数据，结合医院诊疗业务规律、环境需求等因素，通过智能优化算法制定能源调控策略（如中央空调分时分区调控、照明系统智能启停）；调控指令通过 5G 网络实时下发至能源控

制终端（如智能空调控制器、智能照明开关），实现能源的精准调控。在能源管理决策环节，云端平台生成多维度能源消耗报表（按科室、按设备、按时段），为管理部门提供能耗分析、成本核算、节能优化等决策支持；同时，通过算力网络实现各院区能源数据的统一管理与协同优化，提升全院能源管理效率。实施后，医院综合能源消耗降低 20% 以上，能源异常消耗预警响应时间缩短至 1 分钟以内，节能改造投资回报周期缩短至 2-3 年。

（三）物资供应链智慧管理场景

借助 5G+RFID+ 物联网技术，构建覆盖“采购 - 存储 - 领用 - 盘点 - 追溯”全流程的物资供应链智慧管理体系，提升物资管理效率与精准度。在物资标识与采集环节，为药品、高值耗材、办公用品等物资贴上 RFID 电子标签，标签内置物资名称、规格、批次、有效期、供应商等信息；在仓库、药房、科室库房部署 RFID 读写器、智能货架、手持终端等设备，通过 5G 网络实现物资信息的实时采集与上传。在仓储管理环节，智能货架通过 RFID 技术实时监测物资库存数量与位置，当物资库存低于阈值时，自动向采购管理系统推送补货提醒；仓库管理人员通过手持终端可快速完成物资入库、出库、移库等操作，数据实时同步至边缘节点与云端平台，避免人工记录误差；同时，通过温湿度传感器实时监测药品、试剂仓库的环境参数，若参数超标，通过 5G 消息实时预警并联动空调、除湿设备进行调控。在领用与追溯环节，科室人员通过 RFID 读写器快速完成物资领用登记，系统自动扣减库存；云端平台记录物资全流程流转数据，实现从供应商到患者的全链路追溯，若出现物资质量问题，可快速定位问题批次与涉及范围。在多院区协同管理场景，通过算力网络实现各院区物资数据的实时共享，云端平台根据各院区物资需求与库存情况，动态调配物资，避免重复采购与物资积压。实施后，医院物资库存周转率提升 40% 以上，物资盘点时间缩短 70%，账实相符率提升至 99% 以上，高值耗材浪费率降低 30%。

（四）环境与安防智慧管控场景

基于 5G+ 视频监控 + 物联网技术，构建环境与安防智慧管控体系，实现关键区域环境精准调控与全院区安全协同防控。在环境管控方面，在手术室、ICU、新生儿科、药房、实验室等关键区域部署温湿度、洁净度、压差、空气质量等传感器，通过 5G 网络实时传输环境参数至边缘节点；边缘节点对数据进行实时分析，若参数偏离标准范围，自动联动空调、新风系统、除湿设备等进行调

控，确保环境符合医疗规范要求；同时，环境数据实时同步至云端平台，生成环境质量报表，为管理部门提供管控依据。在安防管控方面，部署 5G 高清视频监控摄像头覆盖全院区，摄像头具备 AI 智能分析功能（如人员聚集检测、越界检测、遗留物检测、人脸识别），实时采集安防视频数据并传输至边缘节点；边缘节点通过 AI 算法实时分析视频数据，识别异常行为（如陌生人闯入、人员聚集、火灾烟雾），立即推送预警信息至安防管理平台与安保人员终端，同时联动声光报警器、门禁系统等设备进行处置；在应急处置场景，安保人员通过 5G 高清视频实时查看现场情况，通过应急指挥终端与相关部门开展实时协同，提升应急处置效率。此外，通过算力网络实现各院区环境与安防数据的统一管理，构建全院区一体化安全防控体系，提升整体安全管理水平。实施后，医院关键区域环境参数达标率提升至 99.5% 以上，安防异常事件响应时间缩短至 3 分钟以内，突发事件处置效率提升 60%。

三、核心支撑技术与实施成效

（一）核心支撑技术

支撑医院后勤智慧改造的核心通信技术包括 5G(含 NB-IoT)、物联网、WiFi 6、工业互联网等，同时结合边缘计算、算力网络、AI、大数据等技术形成协同支撑体系。5G 技术凭借高带宽、低延迟、广连接特性，实现高清视频、海量传感器数据的实时传输，支撑远程运维、智能调控等场景；NB-IoT 技术满足低功耗、广覆盖、海量终端接入需求，适用于能源采集、环境监测等低速数据传输场景；物联网技术实现后勤终端与设备的泛在连接，为数据采集提供硬件支撑；WiFi 6 技术为院内移动终端（如运维手持终端、安防终端）提供高速无线接入，保障移动办公效率；边缘计算与算力网络实现后勤数据的实时处理、就近响应与全局调度，提升决策与调控的时效性；AI 与大数据技术用于故障诊断、预测性维护、能源优化、异常预警等，提升后勤管理的智能化水平。

（二）典型实施成效

国内多家医院的后勤智慧改造实践取得显著成效：在管理效率方面，后勤运维人员工作效率提升 50% 以上，物资管理、能源管控等业务流程时间缩短 60% 以上，减少了人工投入；在成本控制方面，综合能源消耗降低 20%-30%，物资浪费率降低 30% 以上，后勤运营成本整体降低 25%-40%；在服务质量方面，关

键设施设备故障发生率降低 60% 以上，环境参数达标率提升至 99% 以上，安防事件处置效率提升 60%，为医疗服务提供了稳定可靠的后勤保障；在管理决策方面，实现了后勤数据的可视化展示与实时分析，管理决策从“经验驱动”向“数据驱动”转型，决策精准度显著提升。

（三）应用挑战与优化方向

当前后勤智慧改造面临的核心挑战包括：一是传统设备改造难度大，部分老旧后勤设备缺乏标准化接口，难以接入物联网系统，改造成本高；二是数据整合难度大，各后勤业务系统数据格式不统一，存在“信息孤岛”，影响协同管理效果；三是技术运维能力不足，智慧后勤系统涉及多领域技术，医院缺乏专业运维团队，难以保障系统稳定运行；四是安全风险隐患，海量后勤数据传输与存储过程中，面临数据泄露、设备被攻击等安全风险。优化方向：制定后勤设备标准化改造规范，开发适配老旧设备的接口模块，降低改造难度与成本；建立统一的后勤数据标准与集成平台，实现各系统数据的无缝整合与共享；加强专业技术团队建设，提升系统运维能力，或通过第三方服务外包模式保障运维质量；构建多层次安全防护体系，采用数据加密、访问控制、入侵检测等技术，保障系统与数据安全。

第四节 通信技术驱动的医疗质量管理与动态监督体系创新

一、医疗质量管理现状与监督体系短板

（一）医疗质量管理核心内涵与重要性

医疗质量管理是医院管理的核心内容，涵盖诊疗行为规范、医疗安全保障、护理质量控制、院感防控、医疗技术应用、服务质量提升等多个维度，核心目标是保障医疗安全、提升诊疗效果、优化患者体验。医疗质量直接关系到患者的生命健康，是医院核心竞争力的重要体现，也是医疗行业监管的重点方向。随着医疗技术的快速发展、多院区布局的普及以及患者对医疗服务需求的提升，传统医疗质量管理模式面临诸多挑战，亟需通过技术创新实现转型升级。

（二）传统监督体系核心短板

传统医疗质量监督体系以人工检查、定期考核、事后追溯为主，存在监督滞后、覆盖不全面、效率低下、数据支撑不足等核心短板：一是监督时效性差，传

统模式以事后检查为主，难以实时发现诊疗过程中的质量问题与安全隐患，往往在问题发生后才进行追溯整改，无法及时干预避免不良事件；二是监督覆盖范围有限，人工检查难以覆盖全院所有诊疗环节、所有科室与所有医护人员，易出现监督盲区，尤其是门诊、急诊、手术等动态诊疗场景的监督难度大；三是监督标准不统一，不同检查人员的判断标准存在差异，导致监督结果客观性与公正性不足；四是数据采集与分析能力薄弱，医疗质量相关数据分散在电子病历、HIS、LIS、PACS等多个系统，难以实现实时整合与分析，监督决策缺乏精准数据支撑；五是多院区监督协同不足，各院区独立开展质量监督，标准不统一、数据不共享，难以实现全院区医疗质量的同质化管理。

二、通信技术驱动的医疗质量管理与动态监督体系架构

（一）体系核心设计理念

以“实时感知、动态监督、精准管控、协同提升”为核心设计理念，依托5G、物联网、WiFi 6等新一代通信技术，结合边缘计算、算力网络、AI、大数据等技术，构建全流程、全场景、智能化的医疗质量管理与动态监督体系。通过通信技术实现医疗质量相关数据的实时采集、高速传输与全域共享，打破信息孤岛；通过边缘计算与算力网络实现数据的实时分析与智能预警，提升监督的时效性与精准性；通过全流程动态监督实现从“事后整改”向“事前预警、事中干预、事后优化”的转型；通过多院区数据协同与标准统一，实现全院区医疗质量的同质化管理。

（二）体系核心架构组成

数据采集层：作为体系的基础，通过泛在通信网络连接各类医疗终端与传感器，实现医疗质量相关数据的全维度、实时采集。采集数据类型包括：诊疗过程数据（电子病历、医嘱、检查检验结果、手术记录、会诊记录）、医护行为数据（诊疗操作规范执行情况、手卫生依从性、无菌操作情况）、设备运行数据（医疗设备校准状态、使用参数、故障信息）、环境数据（手术室、ICU等关键区域温湿度、洁净度）、患者反馈数据（满意度评价、投诉建议）。数据采集终端通过5G、WiFi 6、物联网等技术将数据实时传输至边缘节点，确保数据的时效性与完整性。

通信传输层：采用“5G+WiFi 6+光纤”多网络融合架构，为数据传输提供高速、稳定、安全的通道。5G网络负责高清诊疗视频、实时手术数据、海量传感器数

据的高速传输，支撑远程监督、术中动态监控等场景；WiFi 6 网络为院内医护终端、移动监督终端提供高速无线接入，保障移动诊疗与监督效率；光纤网络为边缘节点与云端平台之间的数据传输提供高带宽、低延迟支撑，保障全域数据共享。同时，部署安全网关、数据加密、访问控制等技术，保障数据传输过程中的安全性与隐私性。

边缘计算与算力调度层：在各院区、各核心业务区域部署边缘节点，负责本地医疗质量数据的实时预处理、分析与智能预警；通过轻量化 AI 算法识别诊疗过程中的异常行为、质量隐患（如不合理医嘱、违规操作、设备异常），立即推送预警信息至相关医护人员与管理部门，实现事中实时干预。同时，依托算力网络实现各边缘节点之间的算力协同与数据共享，当某一区域边缘节点算力不足时，自动调度其他区域空闲边缘节点或云端算力进行补充，保障监督分析的连续性与高效性。

云端管控与分析层：部署在总院核心数据中心，由大数据分析平台、AI 训练平台、质量管控平台组成。核心功能包括：全局数据整合与分析，整合各院区医疗质量数据，开展多维度、深层次分析，生成质量报告与优化建议；AI 模型训练与优化，基于海量医疗质量数据训练高精度监督分析模型，轻量化后下发至边缘节点；质量标准统一管理，制定全院统一的医疗质量标准、诊疗规范与监督流程，同步至各院区；多院区协同监督，实现各院区医疗质量数据的统一监控、对比分析与协同优化，推动同质化管理；决策支持，为医院管理部门提供医疗质量全局监控、风险预警、优化决策等支撑服务。

应用服务层：面向医护人员、质量监督人员、管理部门、患者等不同用户，提供个性化应用服务。包括：医护人员端的质量规范推送、实时预警、操作指导等服务；监督人员端的动态监控、异常核查、监督报表生成等服务；管理部门端的全局质量监控、风险评估、决策分析等服务；患者端的诊疗过程透明化查询、满意度评价、意见反馈等服务。

三、通信技术在质量管控与动态监督中的创新应用场景

（一）诊疗过程动态监督与智能预警场景

依托 5G+AI+ 边缘计算技术，实现诊疗过程的全流程动态监督与智能预警。在门诊诊疗场景，通过移动医生工作站实时采集医嘱、处方等数据，传输至边缘

节点；边缘节点通过 AI 算法对方合理性进行实时分析（如药物配伍禁忌、剂量异常、适应症不符），若发现问题立即向医生终端推送预警信息，提醒医生修改；同时，通过视频监控实时监测门诊诊疗行为，AI 算法识别违规诊疗操作（如未核对患者身份、未按规范记录病历），实时预警并记录。在手术场景，通过 5G 高清视频实时采集手术过程，边缘节点通过 AI 算法分析手术操作规范性（如无菌操作执行情况、手术步骤合规性）；同时，实时采集手术设备运行数据、患者生命体征数据，若出现设备异常或患者生命体征波动，立即推送预警信息至手术医生与麻醉医生，保障手术安全；手术数据实时同步至云端，方便质量监督人员远程监督与术后复盘分析。在住院诊疗场景，通过移动护理终端实时采集护理操作数据，边缘节点分析护理操作合规性（如输液规范、导尿管护理规范），识别护理风险并预警；同时，实时监测医嘱执行进度，确保诊疗方案精准落地。实施后，不合理处方率降低 60% 以上，手术操作违规率降低 50%，护理不良事件发生率降低 45%，诊疗质量显著提升。

（二）院感防控全流程动态监督场景

基于 5G+ 物联网 + 边缘计算技术，构建院感防控全流程动态监督体系，实现院感风险的实时感知与精准管控。在人员管控方面，通过物联网技术采集医护人员手卫生执行数据（如手消毒次数、时间）、防护用品穿戴数据，边缘节点实时分析手卫生依从性，若未按规范执行立即预警；通过人脸识别技术监测医护人员进出隔离区域的权限与防护规范，防止交叉感染。在环境管控方面，实时采集手术室、ICU、隔离病房等关键区域的温湿度、洁净度、空气菌落数等数据，通过 5G 网络传输至边缘节点，若参数超标立即预警并联动环境调控设备进行整改；同时，通过 RFID 技术追踪消毒器械、医疗废物的流转过程，确保消毒达标与废物规范处置。在患者管控方面，实时监测住院患者的体温、症状等数据，通过 AI 算法识别院感疑似病例，立即推送预警信息至院感管理部门，及时开展排查与干预。实施后，医护人员手卫生依从性提升至 95% 以上，院感发生率降低 40% 以上，消毒器械合格率提升至 99.8%。

（三）医疗设备质量与安全动态监督场景

借助 5G+ 物联网 + 算力网络技术，实现医疗设备质量与安全的全生命周期动态监督。在设备运行监督方面，通过物联网传感器实时采集医疗设备（如 CT、MRI、手术机器人、监护仪）的运行参数、校准状态、故障信息，通过 5G

网络传输至边缘节点；边缘节点实时分析设备运行状态，若出现参数异常或潜在故障，立即推送预警信息至设备运维人员与使用科室，指导及时检修；同时，基于设备运行数据预测设备故障风险，生成预测性维护计划。在设备使用监督方面，通过 RFID 技术记录设备使用人员、使用时间、使用场景等信息，确保设备由具备资质的人员操作；边缘节点分析设备使用频率与负荷，优化设备调度方案，提升设备利用率。在设备追溯管理方面，通过算力网络实现各院区设备数据的统一管理，记录设备采购、校准、维修、报废等全生命周期数据，实现全流程追溯，确保设备质量符合医疗规范要求。实施后，医疗设备故障发生率降低 50% 以上，设备校准及时率提升至 99%，设备利用率提升 30% 以上，保障了设备使用安全与诊疗质量。

（四）多院区医疗质量同质化监督场景

依托 5G+ 算力网络 + 云端协同技术，构建多院区医疗质量同质化监督体系，实现全院区质量标准统一、数据共享与协同提升。在标准统一方面，云端平台制定全院统一的医疗质量标准、诊疗规范、监督流程，通过 5G 网络同步至各院区边缘节点与医护终端，确保各院区执行统一标准。在数据协同方面，各院区医疗质量数据通过算力网络实时同步至云端平台，实现全域数据整合与共享；云端平台对各院区质量数据进行对比分析，识别各院区质量差异与薄弱环节，生成个性化优化建议，推送至各院区管理部门。在协同监督方面，质量监督人员通过云端平台可实时监控各院区医疗质量状态，对重点问题开展跨院区联合监督与整改；各院区通过平台共享质量管控经验与最佳实践，推动全院区医疗质量同质化提升。实施后，多院区医疗质量达标率差异缩小至 5% 以内，全院区平均医疗质量达标率提升至 98% 以上，患者跨院区就医体验一致性显著提升。

第九章 医院信息化安全与通信安全管理体系建设

第一节 新一代通信技术环境下医疗信息系统安全风险分析

一、新一代通信技术在医疗信息系统中的应用现状

（一）核心通信技术应用场景全景

新一代通信技术以 5G（含 NB-IoT）、WiFi 6、工业互联网、物联网等为核心，已深度融入医疗信息系统的全流程架构，形成覆盖“终端接入 - 数据传输 - 算力处理 - 业务应用”的全链路支撑体系。在终端接入层面，5G 与 WiFi 6 技术实现了移动医疗终端（如移动医生工作站、护理终端）、物联网感知设备（如温湿度传感器、医疗设备监控终端）、远程医疗设备（如远程手术机器人、高清会诊终端）的高速无线接入，打破了传统有线网络的空间限制，支撑诊疗服务向床旁、院前、社区等场景延伸；NB-IoT 技术则凭借低功耗、广连接特性，实现了对海量低速率医疗物联网设备的长期稳定接入，如慢病监测设备、能源计量终端等。在数据传输层面，5G 的高带宽特性支撑了高清医学影像、手术实时视频、多参数生命体征流等大流量数据的高速传输，保障了远程会诊、术中指导等实时业务的流畅性；多网络融合架构（5G+WiFi 6+ 光纤）则通过智能切换机制，提升了数据传输的稳定性与冗余备份能力。在算力处理层面，通信技术与边缘计算、算力网络的协同，实现了医疗数据的就近处理与全局调度，边缘节点通过高速通信网络承接本地实时数据处理任务，云端则通过骨干通信网络实现全域数据整合与深度分析。在业务应用层面，通信技术驱动了远程医疗、智慧后勤、动态质量监督、多院区协同等创新业务模式的落地，使医疗信息系统从传统的院内管理系统升级为全域协同的智慧医疗服务平台。

具体应用场景中，5G+ 远程医疗已成为优质医疗资源下沉的重要载体，通过 5G 高清视频与低延迟传输，实现了跨区域远程会诊、远程手术指导、远程超声诊断等业务，如某省远程医疗平台通过 5G 网络连接省级三甲医院与县级医院，使基层患者无需转诊即可享受专家诊疗服务；WiFi 6 则广泛应用于院内门诊、住

院楼等区域，为医护人员的移动办公与患者的自助服务提供高速网络支撑，如门诊区域的自助挂号缴费终端、住院楼的床旁结算终端均通过 WiFi 6 实现与核心系统的快速数据交互；物联网与 NB-IoT 技术则构建了全院区的智能感知网络，覆盖医疗设备运维、环境管控、院感防控等多个领域，如通过物联网传感器实时监测手术室温湿度、通过 NB-IoT 终端采集各科室能耗数据。这些应用场景的落地，极大提升了医疗服务效率与质量，但也使医疗信息系统的网络边界从传统的院内有线网络扩展至泛在的无线与物联网环境，安全风险的传播路径与影响范围显著扩大。

（二）医疗信息系统架构演变与安全边界拓展

新一代通信技术的融入推动医疗信息系统架构从传统的“集中式封闭架构”向“分布式开放架构”转型，架构演变呈现三大特征：一是终端层泛在化，接入终端从传统的台式电脑、服务器扩展至移动终端、物联网设备、医疗专用设备等多元化终端，终端数量呈指数级增长；二是网络层扁平化，传统的多层网络架构（核心层 - 汇聚层 - 接入层）逐渐简化，通过 5G、WiFi 6 等技术实现终端与核心系统、边缘节点的直接高速连接，网络拓扑结构更趋复杂；三是数据层分布式，数据存储与处理从单一的云端数据中心分散至边缘节点、终端设备，形成“云 - 边 - 端”协同的数据分布模式。架构演变直接导致医疗信息系统的安全边界发生根本性拓展，传统的物理安全边界（如防火墙、机房隔离）已难以覆盖所有安全风险点，形成了“泛在化安全边界”。

具体而言，安全边界拓展体现在三个维度：一是空间边界拓展，从院内机房、楼宇延伸至院前急救车、社区卫生服务中心、患者家庭等外部场景，如患者居家使用的智能慢病监测设备通过 5G 网络接入医院信息系统，使安全边界延伸至家庭环境；二是网络边界模糊化，无线通信网络的开放性使网络接入不再受物理位置限制，攻击者可通过无线信号覆盖范围外的伪装接入点、信号拦截等方式入侵系统，传统基于 IP 地址的边界防护机制失效；三是数据边界多元化，医疗数据在“云 - 边 - 端”之间频繁流转，数据的产生、传输、存储、使用等环节分布在不同节点，每个节点均可能成为安全风险点，数据安全边界从单一的云端存储边界扩展至全链路的数据流转边界。安全边界的拓展使医疗信息系统面临的安全威胁从传统的内部风险为主，转变为“内部风险 + 外部攻击 + 终端漏洞”的多元风险并存格局，安全防护的难度与复杂度显著提升。

二、终端接入层安全风险

（一）移动医疗终端安全风险

移动医疗终端（如移动医生工作站、护理终端、手持超声仪）是新一代通信技术环境下医疗信息系统的核心接入终端，其安全风险主要体现在设备自身漏洞、接入认证缺陷、数据存储安全三个方面。在设备自身漏洞方面，部分移动医疗终端为追求便携性与低成本，采用简化的操作系统（如定制化 Android 系统），未进行充分的安全加固，存在大量系统漏洞，如操作系统内核漏洞、应用程序权限管理漏洞等；攻击者可通过这些漏洞植入恶意代码，控制终端设备，窃取终端内存储的患者诊疗数据、医护人员账号密码等敏感信息。例如，某品牌移动护理终端因 Android 系统未及时更新安全补丁，被攻击者利用漏洞植入木马程序，导致多个科室的患者生命体征数据泄露。

在接入认证缺陷方面，部分移动医疗终端采用弱认证机制，如静态密码认证、无二次认证等，易被攻击者破解或冒用。医护人员为方便操作，往往设置简单密码（如生日、手机号后六位），或多人共用同一账号，进一步降低了认证安全性；攻击者可通过暴力破解、密码嗅探等方式获取账号密码，伪装成合法用户接入医疗信息系统，篡改诊疗数据、伪造医嘱等，引发医疗安全事故。此外，移动终端的移动性导致设备丢失或被盗风险较高，若终端未开启加密存储功能，攻击者可直接获取终端内的敏感数据；即使开启加密存储，攻击者也可能通过技术手段破解加密，造成数据泄露。

在数据存储安全方面，移动医疗终端需本地存储部分诊疗数据（如离线状态下的患者信息、诊疗记录），但部分终端缺乏完善的数据加密存储机制，敏感数据以明文形式存储在终端内存或存储卡中；同时，终端应用程序的权限管理不严格，部分第三方应用可违规获取终端存储的敏感数据。例如，某移动医生工作站的配套 APP 因权限管理漏洞，被第三方统计应用获取了患者姓名、病历号、诊断结果等核心数据，引发隐私泄露事件。此外，移动终端的数据备份与恢复机制不完善，设备故障或数据被篡改时，无法快速恢复数据，影响医疗业务连续性。

（二）医疗物联网设备安全风险

医疗物联网设备（如温湿度传感器、医疗设备监控终端、智能输液泵、慢病监测设备）数量庞大、类型多样，且大多采用低功耗、轻量化设计，其安全风险

更为突出,主要表现为固件漏洞、默认凭证滥用、缺乏安全通信机制三个方面。在固件漏洞方面,医疗物联网设备的固件开发往往侧重于功能实现,忽视安全防护,存在大量未修复的漏洞,如缓冲区溢出漏洞、命令注入漏洞等;攻击者可通过网络远程利用这些漏洞篡改固件程序,控制设备运行状态,甚至导致设备瘫痪。例如,某品牌智能输液泵的固件存在命令注入漏洞,攻击者可通过网络发送恶意指令,修改输液速度,严重威胁患者生命安全。

在默认凭证滥用方面,绝大多数医疗物联网设备出厂时配备默认管理员账号密码(如 admin/admin、root/root),且部分设备不支持修改默认凭证,或修改流程复杂,导致大量设备长期使用默认凭证;攻击者可通过扫描网络中的物联网设备,利用默认凭证登录设备,获取设备控制权,进而入侵医疗信息系统核心网络。例如,某医院的环境监测传感器网络因设备均使用默认密码,被攻击者批量登录控制,通过传感器网络作为跳板,入侵了医院的 HIS 系统,窃取了大量患者挂号缴费数据。此外,部分物联网设备缺乏身份标识与准入控制机制,攻击者可伪造物联网设备接入网络,发送虚假数据,干扰医疗业务正常运行,如伪造手术室温湿度数据,导致手术环境调控异常。

在缺乏安全通信机制方面,医疗物联网设备与边缘节点、云端平台之间的通信大多采用未加密的明文传输协议(如 HTTP、TCP/UDP),攻击者可通过网络嗅探、中间人攻击等方式拦截传输数据,窃取敏感信息(如设备运行参数、患者监测数据),或篡改数据内容,误导医疗决策。例如,某慢病管理平台的智能血压计通过 NB-IoT 网络传输患者血压数据时采用明文传输,被攻击者拦截获取了数千名患者的身份信息与血压数据;同时,攻击者还篡改了部分患者的血压数据,导致医生做出错误的诊疗判断。此外,物联网设备的通信协议缺乏完整性校验机制,无法发现数据被篡改,进一步加剧了安全风险。

(三) 远程医疗设备安全风险

远程医疗设备(如远程手术机器人、高清会诊终端、远程超声探头)是 5G 技术在医疗领域的核心应用载体,其安全风险直接关系到患者生命安全,主要集中在实时控制安全、数据传输安全、设备协同安全三个方面。在实时控制安全方面,远程手术机器人、远程超声设备等需要通过 5G 网络实现远程实时控制,对网络延迟与稳定性要求极高;攻击者可通过网络攻击(如 DDoS 攻击、干扰攻击)破坏网络传输稳定性,导致控制指令延迟或丢失,引发手术失误、诊断偏差等严

重医疗事故。例如，某远程手术机器人在手术过程中遭遇 DDoS 攻击，网络延迟从 10 毫秒骤增至 500 毫秒，导致手术器械操作失控，造成患者二次伤害。此外，远程控制协议若存在漏洞，攻击者可篡改控制指令，如修改手术机器人的操作轨迹、调整远程超声探头的位置，直接威胁患者安全。

在数据传输安全方面，远程医疗设备传输的高清手术视频、会诊影像、患者诊疗数据等均为核心敏感信息，若传输过程缺乏高强度加密保护，易被攻击者拦截窃取。部分远程医疗设备采用的加密算法存在安全缺陷（如过时的 DES 算法），或加密密钥管理不当（如密钥明文存储、共享使用），无法有效抵御攻击；攻击者可通过破解加密算法、窃取加密密钥等方式获取传输数据，侵犯患者隐私。例如，某远程会诊平台因采用过时的加密算法，被攻击者破解了传输链路，获取了多台会诊终端传输的肿瘤患者影像数据与诊断报告，造成严重的隐私泄露事件。同时，远程医疗数据传输量大，易被攻击者利用作为流量攻击的载体，进一步威胁网络安全。

在设备协同安全方面，远程医疗业务需要多设备协同工作（如会诊终端、医疗影像系统、电子病历系统），设备之间的接口缺乏统一的安全标准，存在接口漏洞与数据格式不兼容问题。攻击者可利用接口漏洞入侵协同设备，获取更多敏感数据，或破坏设备之间的协同工作流程。例如，某远程超声诊断系统与医院 PACS 系统的接口存在权限管理漏洞，攻击者通过该接口入侵 PACS 系统，窃取了大量患者的影像数据；同时，攻击者还篡改了接口数据传输格式，导致远程超声诊断结果无法正常同步至 PACS 系统，影响诊疗业务开展。此外，远程医疗设备的接入权限管理不严格，缺乏精细化的权限控制策略，易导致未授权设备接入协同网络，引发安全风险。

三、网络传输层安全风险分析

（一）5G 网络通信安全风险

5G 网络作为新一代通信技术的核心，在为医疗信息系统提供高速、低延迟传输服务的同时，也带来了新的安全风险，主要包括网络切片安全、核心网安全、终端接入鉴权安全三个方面。在网络切片安全方面，5G 网络通过网络切片技术为不同医疗业务（如远程手术、远程会诊、物联网监测）划分独立的虚拟网络，实现业务隔离；但切片之间的隔离机制若存在缺陷，攻击者可通过切片间的漏洞

进行跨切片攻击，从低安全等级切片（如物联网监测切片）入侵高安全等级切片（如远程手术切片），威胁核心医疗业务安全。例如，攻击者利用物联网监测切片的设备漏洞入侵切片网络，通过切片间的接口漏洞进入远程手术切片，干扰手术控制指令传输。此外，网络切片的资源调度机制若存在安全缺陷，攻击者可通过资源耗尽攻击占用切片网络资源，导致医疗业务无法正常运行。

在核心网安全方面，5G 核心网采用软件定义网络（SDN）、网络功能虚拟化（NFV）等技术，网络功能模块化、虚拟化，使攻击面显著扩大。核心网中的网络功能实体（如 AMF、SMF、UPF）若存在软件漏洞，攻击者可通过远程攻击控制这些实体，窃取用户数据、篡改网络配置、中断网络服务。例如，5G 核心网的 AMF（接入和移动管理功能）实体若存在权限管理漏洞，攻击者可伪造终端身份信息接入核心网，获取医疗信息系统的核心数据；UPF（用户面功能）实体若被攻击控制，可拦截、篡改终端与核心系统之间的传输数据。同时，5G 核心网与传统网络的互联互通接口缺乏完善的安全防护机制，攻击者可通过这些接口从传统网络入侵 5G 核心网，扩大攻击范围。

在终端接入鉴权安全方面，5G 网络采用的鉴权机制（如 AKA 鉴权）虽然相比 4G 有所提升，但仍存在安全缺陷。攻击者可通过伪基站攻击、身份伪造等方式绕过鉴权机制，伪装成合法终端接入 5G 网络；或通过中间人攻击拦截鉴权信息，破解鉴权密钥，获取网络接入权限。例如，攻击者在医院周边部署伪 5G 基站，诱导移动医疗终端接入伪基站，进而窃取终端传输的敏感数据，或向终端推送恶意指令。此外，5G 终端的 SIM 卡若存在漏洞，攻击者可复制 SIM 卡，实现身份冒用，接入医疗信息系统网络。

（二）WiFi 6 网络安全风险

WiFi 6 网络因高带宽、低延迟、多设备接入特性，广泛应用于院内移动办公与患者服务场景，但仍存在传统无线网络的安全隐患，同时新增了部分新的安全风险，主要包括加密机制缺陷、接入点安全、漫游安全三个方面。在加密机制缺陷方面，部分医院为兼容老旧终端，仍采用过时的 WiFi 加密协议（如 WEP、WPA），这些协议存在严重安全漏洞，易被攻击者破解；即使采用 WiFi 6 推荐的 WPA3 加密协议，若配置不当（如使用弱密钥、未开启强制加密），也会降低加密安全性。攻击者可通过破解加密密钥接入 WiFi 网络，窃取网络内传输的医疗数据，或发起中间人攻击，篡改数据内容。例如，某医院门诊区域的 WiFi 网

络因采用 WPA 加密协议，被攻击者破解密钥后接入网络，嗅探获取了医护人员移动终端传输的患者诊疗数据与账号密码。

在接入点安全方面，WiFi 6 接入点（AP）的固件若存在漏洞，攻击者可通过远程攻击控制 AP，篡改网络配置、植入恶意代码，或利用 AP 作为跳板入侵医疗信息系统核心网络。部分医院的 WiFi AP 未及时更新安全补丁，或采用默认管理员账号密码，进一步加剧了安全风险。此外，医院内部存在大量私接 AP 的情况，医护人员为方便个人设备接入，私自部署无线路由器，这些私接 AP 未经过安全检测，缺乏必要的安全防护措施，易被攻击者利用作为入侵入口。例如，某科室医护人员私接的 WiFi AP 被攻击者控制，通过该 AP 入侵了科室内部的医疗设备管理系统，窃取了医疗设备运行数据。

在漫游安全方面，WiFi 6 支持终端在不同 AP 之间快速漫游，以保障移动办公的连续性，但漫游过程中的身份认证与数据传输存在安全风险。终端在漫游切换 AP 时，需重新进行身份认证，若认证机制不严密，攻击者可利用漫游间隙进行身份伪造，接入网络；同时，漫游过程中数据传输可能出现短暂的加密中断，攻击者可利用这一间隙拦截传输数据。例如，医护人员携带移动护理终端在住院楼不同楼层之间移动时，终端在 AP 之间漫游切换，攻击者利用漫游认证间隙伪造终端身份接入网络，获取了终端传输的患者生命体征数据。此外，WiFi 6 网络的多用户 MIMO 技术可能导致用户数据之间的干扰，若缺乏完善的隔离机制，可能造成数据泄露。

（三）多网络融合安全风险

新一代通信技术环境下，医疗信息系统采用“5G+WiFi 6+ 光纤 + 物联网”的多网络融合架构，实现了不同网络的优势互补，但也使网络之间的安全边界更加模糊，产生了新的融合安全风险，主要包括网络边界穿透、数据流转安全、网络管理混乱三个方面。在网络边界穿透方面，多网络融合架构中，不同网络之间通过网关、路由器等设备互联互通，若这些互联互通设备存在安全漏洞，或访问控制策略配置不当，攻击者可通过低安全等级网络（如物联网网络）穿透至高安全等级网络（如核心业务网络）。例如，攻击者通过物联网传感器网络的漏洞入侵网络，利用网络融合网关的访问控制缺陷，进入医院核心业务网络，篡改 HIS 系统中的诊疗数据。此外，多网络融合导致网络拓扑结构复杂，攻击者可利用网络间的路由转发机制，隐藏攻击路径，增加攻击检测与溯源的难度。

在数据流转安全方面,医疗数据在多网络之间频繁流转(如从 5G 网络的移动终端流转至光纤网络的核心系统,再流转至 WiFi 6 网络的门诊终端),数据流转过程中的加密机制不统一,存在数据解密后重新加密的中间环节,易被攻击者利用窃取数据。例如,患者诊疗数据从移动护理终端通过 5G 网络传输至边缘节点时采用 AES 加密,边缘节点解密后传输至核心系统时采用 DES 加密,攻击者在边缘节点与核心系统之间的传输链路拦截数据,利用 DES 加密的漏洞破解数据。同时,数据流转过程中缺乏完善的完整性校验与追溯机制,无法有效发现数据被篡改,也难以追溯数据流转路径,一旦发生数据安全事件,无法快速定位责任主体。

在网络管理混乱方面,多网络融合架构涉及多种网络技术与设备,需要统一的网络管理平台进行管控,但部分医院缺乏完善的网络管理体系,不同网络由不同部门独立管理,导致网络配置不一致、安全策略不统一。例如,5G 网络由信息科管理,WiFi 6 网络由后勤部门管理,物联网网络由设备科管理,各部门的安全防护标准不同,形成“安全孤岛”;攻击者可利用不同网络之间的安全策略差异,从安全防护薄弱的网络入手,入侵整个医疗信息系统。此外,网络管理平台若存在安全漏洞,攻击者可控制管理平台,获取所有网络的配置信息与访问权限,全面入侵网络系统,造成毁灭性打击。

(四) 物联网通信协议安全风险

医疗物联网设备广泛采用的通信协议(如 MQTT、CoAP、LoRa、NB-IoT)大多为轻量化协议,设计初衷侧重于低功耗、低带宽,缺乏完善的安全机制,存在显著的安全风险。在 MQTT 协议安全方面,MQTT 协议采用简单的用户名/密码认证机制,认证强度低,易被破解;同时,协议缺乏数据加密传输机制,默认采用明文传输,攻击者可通过网络嗅探获取传输数据,或通过中间人攻击篡改数据。例如,某医院的智能输液泵通过 MQTT 协议与边缘节点传输数据,因未开启加密功能,被攻击者拦截获取了输液参数与患者信息,同时篡改了输液速度参数。此外,MQTT 协议的主题订阅机制若存在权限管理缺陷,攻击者可订阅未授权的主题,获取其他设备的传输数据。

在 CoAP 协议安全方面,CoAP 协议采用 UDP 作为传输层协议,UDP 协议本身不提供可靠性保障与流量控制,攻击者可通过 UDP 洪水攻击导致 CoAP 服务器瘫痪;同时,CoAP 协议的安全扩展机制(如 DTLS)配置复杂,部分医疗

物联网设备未开启 DTLS 加密,导致数据传输安全无法保障。例如,某医院的环境监测传感器采用 CoAP 协议传输数据,未开启 DTLS 加密,攻击者通过 UDP 洪水攻击瘫痪了传感器数据采集服务器,导致环境监测业务中断。此外,CoAP 协议的资源访问控制机制不完善,攻击者可通过暴力猜测资源 URI,访问未授权的设备资源,获取敏感数据。

在 LoRa 与 NB-IoT 协议安全方面,LoRa 网络采用扩频通信技术,信号覆盖范围广,但加密机制简单,采用 AES-128 加密算法,若密钥管理不当(如统一密钥、密钥泄露),易被攻击者破解;攻击者可通过监听 LoRa 信号,破解加密数据,或伪造 LoRa 网关,欺骗物联网设备接入,获取设备数据。NB-IoT 网络由运营商部署,医院难以对网络传输过程进行直接安全管控,若运营商的 NB-IoT 网络存在安全漏洞,或数据传输链路缺乏端到端加密,易导致患者数据泄露。例如,某慢病管理平台的 NB-IoT 血压计数据在传输至运营商网络时,因链路未加密,被攻击者拦截获取了患者的身份信息与血压数据。

四、算力处理层安全风险分析

(一) 边缘节点安全风险

边缘节点作为“云-边-端”协同架构的核心环节,承担着本地医疗数据实时处理、缓存与转发功能,其安全风险直接影响医疗业务的实时性与数据安全性,主要体现在节点硬件安全、软件平台安全、数据缓存安全三个方面。在节点硬件安全方面,边缘节点大多部署在医院各楼层、门诊楼、住院楼等分散区域,物理安全防护措施薄弱,易被攻击者物理接触;攻击者可通过拆卸硬件、接入外接设备(如 U 盘、移动硬盘)等方式,窃取节点内的敏感数据,或植入恶意硬件(如木马芯片),控制边缘节点。例如,某医院门诊楼的边缘节点因未部署物理安全防护装置,被攻击者物理接触后植入恶意芯片,导致节点内缓存的患者诊疗数据被窃取。此外,边缘节点的硬件设备若存在固件漏洞,攻击者可通过远程攻击篡改固件,破坏节点正常运行。

在软件平台安全方面,边缘节点采用的边缘计算平台(如 Kubernetes Edge、EdgeX Foundry)若存在软件漏洞,攻击者可通过远程攻击控制平台,窃取数据或破坏业务流程。边缘计算平台的容器化部署模式使容器镜像成为新的攻击面,若容器镜像未经过安全检测,存在恶意代码或漏洞,攻击者可通过容器入侵边缘

节点。例如，某医院边缘节点使用的容器镜像存在漏洞，被攻击者利用入侵容器，进而突破容器隔离机制，控制整个边缘节点。此外，边缘计算平台的权限管理机制若不完善，攻击者可通过提升权限获取节点的最高控制权，篡改节点配置，中断医疗数据处理业务。

在数据缓存安全方面，边缘节点需要缓存大量本地医疗数据（如患者实时诊疗数据、医疗设备运行数据），若缓存数据未采用加密存储，或加密密钥管理不当，攻击者可直接获取缓存数据；同时，边缘节点的缓存数据同步机制若存在安全缺陷，攻击者可篡改缓存数据，导致同步至云端的数据失真，影响医疗决策。例如，某医院边缘节点缓存的手术实时数据未加密存储，被攻击者窃取；同时，攻击者还篡改了部分缓存数据，导致云端平台获取的手术数据不准确，影响了远程手术指导的安全性。此外，边缘节点的缓存数据清理机制不完善，过期数据未及时清理，增加了数据泄露的风险。

（二）算力网络调度安全风险

算力网络调度系统负责医疗信息系统“云-边-端”算力资源的动态分配与调度，其安全风险直接影响算力资源的可用性与数据处理的安全性，主要包括调度算法安全、调度平台安全、算力节点协同安全三个方面。在调度算法安全方面，算力调度算法若存在逻辑漏洞，攻击者可通过构造恶意任务请求，误导调度系统分配错误的算力资源，导致核心医疗业务算力不足，或使算力资源被恶意占用。例如，攻击者向算力调度系统提交大量伪造的高优先级医疗数据处理任务，导致调度系统将大部分算力资源分配给这些虚假任务，真实的远程手术、急诊数据处理任务因算力不足而延迟，引发医疗安全事故。此外，调度算法的机器学习模型若被攻击者污染，可导致调度决策偏差，影响算力资源的优化配置。

在调度平台安全方面，算力调度平台作为算力网络的核心管控节点，若存在软件漏洞或配置缺陷，攻击者可通过远程攻击控制平台，获取所有算力节点的配置信息与访问权限，篡改调度策略，中断算力资源分配。例如，某医院算力调度平台的 Web 管理界面存在 SQL 注入漏洞，被攻击者利用获取了平台管理员权限，进而控制了整个算力网络，导致各边缘节点与云端的算力协同中断。同时，调度平台的用户认证与权限管理机制若不完善，攻击者可通过破解账号密码、权限提升等方式获取平台控制权，引发安全风险。此外，调度平台的日志管理机制若不健全，无法记录算力调度的全流程操作，一旦发生安全事件，难以追溯攻击源头。

在算力节点协同安全方面，算力网络中的边缘节点、云端节点之间通过协同协议实现算力资源共享与任务分发，若协同协议存在安全漏洞，攻击者可利用漏洞伪造协同请求，获取其他节点的算力资源，或窃取节点间传输的敏感数据。例如，攻击者伪造边缘节点的协同请求，向云端节点申请算力资源，获取云端节点的访问权限，进而窃取云端存储的核心医疗数据。同时，算力节点之间的身份认证机制若不严密，攻击者可伪造算力节点接入算力网络，参与算力调度，破坏算力网络的稳定性与安全性。此外，算力节点的负载均衡机制若存在缺陷，攻击者可通过负载攻击导致部分节点过载瘫痪，影响整个算力网络的正常运行。

（三）云端数据中心安全风险

云端数据中心是医疗信息系统的核心数据存储与算力处理中心，汇聚了海量患者诊疗数据、医疗业务数据，其安全风险具有影响范围广、危害程度大的特点，主要包括存储安全、虚拟化安全、访问控制安全三个方面。在存储安全方面，云端数据中心采用的存储设备（如 SAN、NAS）若存在硬件漏洞，或存储介质（如硬盘、SSD）存在损坏风险，可能导致数据丢失或损坏；同时，存储数据若未采用加密存储（如静态数据加密、传输数据加密），或加密密钥管理不当，易被攻击者窃取。例如，某医院云端数据中心的存储设备因未开启静态数据加密，被攻击者入侵后窃取了数百万条患者诊疗数据。此外，数据备份与恢复机制若不完善，数据发生丢失或损坏时无法快速恢复，影响医疗业务连续性。

在虚拟化安全方面，云端数据中心广泛采用虚拟化技术（如 VMware、KVM）部署服务器，虚拟化层的安全漏洞成为新的攻击面。攻击者可通过虚拟化层漏洞进行跨虚拟机攻击，从一个低安全等级的虚拟机入侵高安全等级的虚拟机，窃取核心数据。例如，攻击者利用虚拟化层的漏洞，从部署普通办公系统的虚拟机入侵部署 HIS 系统的虚拟机，获取了患者挂号缴费数据与医护人员账号密码。同时，虚拟机关机、迁移过程中的数据安全防护不足，易导致数据泄露；虚拟机镜像若存在漏洞或恶意代码，可被攻击者利用入侵整个虚拟化环境。此外，虚拟化管理平台若存在安全缺陷，攻击者可控制管理平台，对虚拟机进行任意操作，破坏云端数据中心的正常运行。

新一代通信技术驱动的创新医疗应用（如远程医疗平台、AI 辅助诊断系统、慢病管理 APP）在提升医疗服务效率的同时，也带来了新的安全风险，主要包括应用程序漏洞、数据共享安全、用户隐私保护不足三个方面。在应用程序漏洞方

面,远程医疗平台、慢病管理 APP 等应用程序的开发周期较短,安全测试不充分,存在大量安全漏洞,如客户端漏洞、服务器端漏洞、API 接口漏洞等。攻击者可利用这些漏洞入侵应用程序,窃取用户数据或控制应用功能。例如,某慢病管理 APP 的 API 接口存在权限管理漏洞,攻击者可通过该接口获取所有注册用户的身份信息、慢病监测数据等敏感数据。同时,移动 APP 的签名机制若存在缺陷,攻击者可篡改 APP 代码,植入恶意代码后重新打包发布,诱导用户下载安装,窃取用户数据。

医疗信息系统通过 API 接口接入大量第三方服务(如医保结算服务、药品配送服务、第三方支付服务、AI 算法服务),第三方服务的安全风险可通过接口渗透至医疗信息系统,主要包括接口安全、第三方服务自身安全、数据交互安全三个方面。在接口安全方面,医疗信息系统与第三方服务之间的 API 接口若存在安全漏洞(如未授权访问、参数篡改、接口滥用),攻击者可利用这些漏洞入侵医疗信息系统,窃取数据或破坏业务流程。例如,某医院的医保结算接口存在未授权访问漏洞,攻击者可通过该接口伪造医保结算数据,骗取医保基金。同时,接口的认证与加密机制不完善,如采用静态密钥认证、数据明文传输,易被攻击者破解,导致接口被滥用。此外,接口的访问频率限制与流量控制机制缺失,攻击者可通过接口进行暴力攻击或流量攻击,导致系统瘫痪。

在访问控制安全方面,云端数据中心的访问控制机制若存在缺陷,攻击者可通过未授权访问、权限提升等方式获取数据中心的访问权限。部分医院的云端数据中心采用弱口令认证、缺乏多因素认证机制,易被攻击者破解账号密码;同时,权限分配不合理,部分用户拥有超出其业务需求的权限,增加了数据泄露的风险。例如,某医院云端数据中心的一名普通运维人员因权限分配过大,可访问所有患者诊疗数据,最终因个人原因窃取并泄露了大量敏感数据。此外,云端数据中心的远程访问接口若缺乏安全防护,攻击者可通过远程攻击接口入侵数据中心,引发严重安全事件。

五、应用服务层安全风险分析

(一) 医疗核心业务系统安全风险

在数据泄露方面,医疗核心业务系统存储的患者诊疗数据、医护人员信息等均为高度敏感数据,若系统的数据安全防护机制不完善,易发生数据泄露。部分

系统的数据传输采用明文传输，或加密机制存在缺陷，攻击者可通过网络嗅探获取传输数据；系统的数据库若未进行安全加固，存在弱口令、权限管理混乱等问题，攻击者可直接入侵数据库窃取数据。例如，某医院的 PACS 系统数据库采用弱口令认证，被攻击者破解后入侵数据库，窃取了大量患者的医学影像数据与诊断报告。此外，系统的日志审计机制不完善，无法及时发现数据访问异常行为，导致数据泄露事件难以被及时察觉。

医疗核心业务系统（如 HIS、LIS、PACS、EMR）是医疗信息系统的核心组成部分，存储与处理大量敏感医疗数据，其安全风险直接关系到医疗业务的正常开展与患者隐私保护，主要包括系统漏洞、数据泄露、业务逻辑漏洞三个方面。在系统漏洞方面，部分医疗核心业务系统采用老旧的开发框架与技术，未及时进行安全升级，存在大量已知漏洞（如 SQL 注入、XSS 跨站脚本、文件上传漏洞）；攻击者可利用这些漏洞入侵系统，窃取数据或破坏业务流程。例如，某医院的 HIS 系统因存在 SQL 注入漏洞，被攻击者利用获取了系统管理员权限，窃取了患者姓名、身份证号、诊疗记录等核心数据。同时，系统开发商提供的补丁更新不及时，或医院未及时部署补丁，进一步加剧了漏洞被利用的风险。

在业务逻辑漏洞方面，医疗核心业务系统的业务逻辑若存在设计缺陷，攻击者可利用这些缺陷进行恶意操作，引发医疗安全事故或数据泄露。例如，HIS 系统的医嘱管理模块若存在逻辑漏洞，攻击者可伪造医生医嘱，修改患者用药信息，威胁患者生命安全；EMR 系统的病历修改模块若存在逻辑漏洞，攻击者可篡改患者的诊疗记录，影响医疗纠纷的责任认定。同时，系统的业务流程缺乏必要的校验机制，如患者身份认证不严格、医嘱执行缺乏二次确认，易被攻击者利用进行违规操作。此外，多系统之间的接口集成若存在逻辑漏洞，攻击者可通过接口调用获取未授权数据，或破坏系统之间的业务协同。

（二）创新医疗应用安全风险

在数据共享安全方面，AI 辅助诊断系统、远程医疗平台等创新应用需要跨系统、跨机构共享医疗数据，以实现算法训练与业务协同，但数据共享过程中缺乏完善的安全机制，易发生数据泄露。部分应用采用明文传输共享数据，或数据脱敏不彻底，导致敏感数据被泄露；数据共享的权限管理机制不完善，未授权机构或个人可获取共享数据。例如，某 AI 辅助诊断系统在与多家医院共享医疗影像数据时，因数据脱敏不彻底，泄露了患者的身份信息与完整诊疗记录。此外，

数据共享过程中缺乏数据流转追溯机制，无法监控数据的使用范围，易导致数据被滥用。

借助 5G+ 物联网 + 算力网络技术，实现医疗设备质量与安全的全生命周期动态监督。在设备运行监督方面，通过物联网传感器实时采集医疗设备（如 CT、MRI、手术机器人、监护仪）的运行参数、校准状态、故障信息，通过 5G 网络传输至边缘节点；边缘节点实时分析设备运行状态，若出现参数异常或潜在故障，立即推送预警信息至设备运维人员与使用科室，指导及时检修；同时，基于设备运行数据预测设备故障风险，生成预测性维护计划。在设备使用监督方面，通过 RFID 技术记录设备使用人员、使用时间、使用场景等信息，确保设备由具备资质的人员操作；边缘节点分析设备使用频率与负荷，优化设备调度方案，提升设备利用率。在设备追溯管理方面，通过算力网络实现各院区设备数据的统一管理，记录设备采购、校准、维修、报废等全生命周期数据，实现全流程追溯，确保设备质量符合医疗规范要求。实施后，医疗设备故障发生率降低 50% 以上，设备校准及时率提升至 99%，设备利用率提升 30% 以上，保障了设备使用安全与诊疗质量。

在用户隐私保护不足方面，创新医疗应用往往需要收集大量用户隐私数据（如患者的位置信息、健康数据、生活习惯数据），但部分应用的隐私政策不透明，未明确告知用户数据收集的范围与用途；同时，数据收集后缺乏必要的安全防护措施，易被攻击者窃取。例如，某远程医疗 APP 违规收集用户的位置信息与手机通讯录数据，且未对这些数据进行加密存储，被攻击者入侵后导致数据泄露。此外，部分应用存在过度收集数据的问题，收集与业务无关的用户隐私数据，增加了隐私泄露的风险。

（三）第三方服务接入安全风险

在第三方服务自身安全方面，部分第三方服务提供商的安全防护能力薄弱，其系统若存在安全漏洞，攻击者可通过入侵第三方服务系统，再通过接口渗透至医疗信息系统。例如，某第三方药品配送服务系统被攻击者入侵，获取了与医院信息系统对接的接口密钥，进而通过该密钥入侵了医院的药品管理系统，窃取了药品采购与库存数据。同时，第三方服务提供商的内部人员若缺乏安全意识，可能泄露医疗信息系统的接口信息与敏感数据；第三方服务的运维管理不规范，也可能导致安全风险。此外，部分第三方服务采用开源组件开发，开源组件存在的

漏洞也可能被攻击者利用，引发安全事件。

依托 5G+ 算力网络 + 云端协同技术，构建多院区医疗质量同质化监督体系，实现全院区质量标准统一、数据共享与协同提升。在标准统一方面，云端平台制定全院统一的医疗质量标准、诊疗规范、监督流程，通过 5G 网络同步至各院区边缘节点与医护终端，确保各院区执行统一标准。在数据协同方面，各院区医疗质量数据通过算力网络实时同步至云端平台，实现全域数据整合与共享；云端平台对各院区质量数据进行对比分析，识别各院区质量差异与薄弱环节，生成个性化优化建议，推送至各院区管理部门。在协同监督方面，质量监督人员通过云端平台可实时监控各院区医疗质量状态，对重点问题开展跨院区联合监督与整改；各院区通过平台共享质量管控经验与最佳实践，推动全院区医疗质量同质化提升。实施后，多院区医疗质量达标率差异缩小至 5% 以内，全院区平均医疗质量达标率提升至 98% 以上，患者跨院区就医体验一致性显著提升。

在数据交互安全方面，医疗信息系统与第三方服务之间的数据交互若缺乏完善的安全机制，易发生数据泄露或篡改。部分数据交互采用明文传输，或加密算法存在缺陷，攻击者可拦截获取交互数据；数据交互过程中缺乏完整性校验机制，无法发现数据被篡改。例如，某医院与第三方支付服务之间的结算数据采用明文传输，被攻击者拦截获取了患者的支付信息与诊疗费用数据。同时，数据交互的范围与权限未进行严格控制，第三方服务可获取超出其业务需求的医疗数据，增加了数据泄露的风险。此外，数据交互完成后，第三方服务未及时清理存储的医疗数据，导致数据长期留存，进一步加剧了安全风险。

六、管理与人员安全风险分析

（一）安全管理制度不完善

部分医院缺乏完善的信息化安全与通信安全管理制度，导致安全防护工作无章可循，主要体现在制度缺失、制度更新不及时、制度执行不到位三个方面。在制度缺失方面，医院未建立覆盖终端管理、网络安全、数据安全、应急处置等全流程的安全管理制度，如缺乏物联网设备管理规范、移动终端安全管理办法、数据分级分类管理规则等，导致部分安全风险点处于无管控状态。例如，某医院因缺乏物联网设备管理规范，大量医疗物联网设备未进行登记备案，存在设备被篡改、冒用的风险。同时，医院未建立安全责任追究制度，安全事件发生后无法明

确责任主体，导致安全管理工作流于形式。

在制度更新不及时方面，随着新一代通信技术的快速发展，医疗信息系统的架构与应用场景不断变化，新的安全风险不断涌现，但医院的安全管理制度未及时更新，仍沿用传统的安全管理模式，无法适应新的安全防护需求。例如，医院针对 5G 网络、边缘计算、算力网络等新技术的安全管理制度缺失，导致这些新技术在应用过程中缺乏必要的安全管控。同时，医院未及时跟进《数据安全法》《个人信息保护法》等相关法律法规的要求，安全管理制度存在合规性缺陷，可能引发法律风险。此外，安全管理制度的更新流程繁琐，无法快速响应新的安全威胁，进一步降低了制度的有效性。

在制度执行不到位方面，部分医院虽然建立了完善的安全管理制度，但缺乏有效的监督与考核机制，导致制度无法落到实处。例如，医院规定移动终端需定期更新安全补丁、设置复杂密码，但部分医护人员未严格执行，仍使用简单密码、未更新补丁，导致移动终端存在安全漏洞。同时，安全管理部门对制度执行情况的检查频率不足，无法及时发现与纠正违规行为；考核机制不完善，对违规人员未进行有效的处罚，无法起到警示作用。此外，医院各部门之间缺乏协同配合，安全管理制度的执行存在“各自为政”的情况，影响了安全管理的整体效果。

（二）人员安全意识薄弱

人员安全意识薄弱是医疗信息系统安全风险的重要诱因，医护人员、运维人员、管理人员等不同岗位人员均可能因安全意识不足引发安全事件，主要体现在违规操作、密码管理不当、轻信钓鱼攻击三个方面。在违规操作方面，部分医护人员为方便工作，存在违规操作行为，如多人共用账号、随意将移动终端借给他人使用、私接网络设备等，这些行为破坏了医院的安全管理规范，为攻击者提供了可乘之机。例如，某科室医护人员多人共用一个移动护理终端账号，导致该账号被盗用后，攻击者可轻易获取多个患者的诊疗数据。同时，部分运维人员进行系统维护时，未严格遵守安全操作流程，如在生产环境中进行未授权的测试操作、泄露系统配置信息，可能导致系统漏洞被利用。

在密码管理不当方面，医护人员、运维人员普遍存在密码设置简单、长期不更换密码、密码复用等问题，导致账号密码易被攻击者破解。例如，部分医护人员将账号密码设置为“123456”“000000”等简单密码，攻击者可通过暴力破解轻松获取账号权限；部分人员在多个系统中使用相同的账号密码，一旦一个系统

的密码泄露，可能导致多个系统的账号被冒用。同时，医院缺乏有效的密码管理工具与强制密码策略，无法强制用户设置复杂密码、定期更换密码，进一步加剧了密码管理的安全风险。此外，部分人员在密码丢失或遗忘后，通过非正规渠道找回密码，未进行严格的身份认证，可能导致密码被他人冒用。

在轻信钓鱼攻击方面，攻击者针对医院人员发起的钓鱼攻击日益频繁，通过伪造邮件、短信、微信消息等方式，诱导人员点击恶意链接、下载恶意附件，进而窃取账号密码或植入恶意代码。由于部分医院人员缺乏钓鱼攻击识别能力，容易轻信这些恶意信息，导致安全事件发生。例如，攻击者伪造医院信息科的邮件，以“系统升级通知”为由，诱导医护人员点击恶意链接，窃取了大量医护人员的账号密码。同时，医院缺乏针对钓鱼攻击的常态化培训，人员无法及时掌握新的钓鱼攻击手段，进一步增加了被攻击的风险。此外，部分人员在收到可疑信息后，未及时向安全管理部门报告，导致攻击范围扩大。

第二节 医疗通信网络的安全防护策略

一、医疗通信网络安全防护体系架构设计

（一）体系架构设计原则

医疗通信网络安全防护体系的构建需立足医疗业务的特殊性与敏感性，遵循“纵深防御、分级防护、协同联动、合规可控”四大核心原则。纵深防御原则要求打破单一防护壁垒，构建覆盖“终端接入 - 网络传输 - 算力节点 - 应用服务”全链路的多层防护体系，通过不同层级防护措施的互补与协同，提升整体防护能力，即使某一层级防护失效，其他层级仍能有效阻挡攻击。分级防护原则基于医疗通信网络中不同业务的安全等级差异，对核心业务（如远程手术、急诊救治）通信链路实施高强度防护，对普通办公、患者自助服务等非核心业务实施差异化防护，实现资源的合理配置与精准防护。协同联动原则强调防护体系内部各组件（如防火墙、入侵检测系统、安全管理平台）之间的信息共享与协同响应，同时建立医院内部信息科、医务科、后勤科等多部门的协同机制，以及与运营商、安全服务商的外部联动机制，确保安全事件发生时能够快速响应、协同处置。合规可控原则要求防护体系的设计与建设严格遵循《网络安全法》《数据安全法》《个

人信息保护法》《医疗卫生机构网络安全管理办法》等相关法律法规与行业标准，确保医疗通信网络的安全运行与医疗数据的合法合规使用，同时建立完善的安全审计与追溯机制，实现对网络行为与安全事件的全程可控。

在具体实践中，上述原则需贯穿防护体系设计的全流程。例如，在纵深防御体系构建中，需在终端接入层部署终端安全管理系统、准入控制系统，在网络传输层部署防火墙、入侵防御系统、VPN 设备，在算力节点层部署数据加密、访问控制设备，在应用服务层部署 Web 应用防火墙、API 网关等，形成多层级、全方位的防护屏障；在分级防护实施中，需先对医疗通信网络中的业务进行安全等级划分，明确核心业务、重要业务、一般业务的范围与安全需求，再针对不同等级业务制定差异化的防护策略，如核心业务通信链路采用加密传输、多因素认证、冗余备份等多重防护措施，一般业务则采用基础的访问控制与安全审计措施。

（二）体系架构核心组成

医疗通信网络安全防护体系架构以“安全感知中心”为核心，构建“终端安全接入域、网络边界防护域、核心网络防护域、算力节点防护域、安全管理与运营域”五大防护域，各防护域相互关联、协同工作，形成完整的安全防护闭环。安全感知中心作为体系的“大脑”，负责收集各防护域的安全日志、告警信息、流量数据等，通过大数据分析、人工智能检测等技术实现对安全威胁的实时感知、精准识别与预警预测，为安全决策与应急处置提供支撑。

终端安全接入域是防护体系的第一道防线，覆盖移动医疗终端、医疗物联网设备、远程医疗设备等所有接入医疗通信网络的终端设备，核心组件包括终端准入控制系统、终端安全管理平台、移动设备管理（MDM）系统等，主要实现对终端设备的身份认证、安全状态检查、漏洞管理、数据加密等功能，确保只有安全合规的终端才能接入网络。网络边界防护域负责保障医疗通信网络与外部网络（如互联网、运营商网络、跨机构协作网络）之间的边界安全，核心组件包括下一代防火墙（NGFW）、入侵防御系统（IPS）、VPN 网关、网络隔离设备等，主要实现边界访问控制、恶意流量拦截、VPN 加密接入、网络隔离等功能，防止外部攻击通过边界渗透至内部网络。核心网络防护域覆盖医院内部核心通信网络（如 5G 核心网、光纤骨干网、WiFi 6 核心网络），核心组件包括网络流量分析系统、链路加密设备、核心路由安全加固设备等，主要实现对核心网络流量的实时监控、通信链路的加密保护、核心网络设备的安全加固等功能，保障核心网

络的稳定运行与数据传输安全。

算力节点防护域覆盖边缘节点、云端数据中心等算力节点，核心组件包括数据加密设备、访问控制服务器、虚拟机安全防护系统等，主要实现对算力节点数据的加密存储与传输、节点访问权限的精细化控制、虚拟化环境的安全防护等功能，保障算力节点的安全运行与数据安全。安全管理与运营域负责对整个防护体系的统一管理与运营，核心组件包括安全信息与事件管理（SIEM）系统、安全编排自动化与响应（SOAR）系统、漏洞管理平台、安全审计系统等，主要实现安全策略的统一配置与管理、安全事件的集中分析与处置、漏洞的全生命周期管理、安全行为的全程审计等功能，提升防护体系的运营效率与管理水平。

（三）与现有信息化体系的融合衔接

医疗通信网络安全防护体系的建设需与医院现有信息化体系（如 HIS、LIS、PACS、电子病历系统等）实现深度融合衔接，避免形成“安全孤岛”，确保安全防护与业务应用协同发展。在网络层面，防护体系需与现有医疗信息系统的网络架构相匹配，充分利用现有网络设备的安全功能，通过接口对接、配置联动等方式实现防护策略与网络架构的协同适配，例如将安全感知中心与现有网络管理平台对接，实现网络拓扑、设备状态、安全事件等信息的共享与联动处置。在数据层面，防护体系需与现有医疗数据管理体系相融合，遵循医院数据分级分类管理规则，针对不同类型、不同等级的医疗数据制定差异化的加密传输与存储策略，确保医疗数据在产生、传输、存储、使用等全流程的安全，例如将数据加密设备与现有电子病历系统、PACS 系统对接，实现医疗影像、诊疗记录等敏感数据的自动加密传输与存储。

在应用层面，防护体系需与现有医疗业务应用系统实现无缝衔接，避免对医疗业务的正常开展造成影响，例如在部署 Web 应用防火墙时，需针对 HIS 系统、远程医疗平台等应用系统的特点进行精准配置，确保既能有效拦截针对应用系统的攻击，又不影响应用系统的响应速度与业务流程；在部署终端安全管理系统时，需充分考虑移动医疗终端、医疗物联网设备的业务特性，避免因安全管控措施过度严格导致设备无法正常开展业务。此外，防护体系还需与医院现有信息化管理制度、流程相融合，将安全管理要求嵌入到现有信息化运维管理、业务操作流程中，例如将终端漏洞修复、安全补丁更新纳入现有信息化运维流程，将安全事件处置流程与现有医疗应急管理流程相衔接，确保安全防护措施的有效落地与执行。

二、终端安全接入防护策略

(一) 终端准入安全防护

终端准入安全防护是保障医疗通信网络安全的基础,核心目标是实现“未授权终端不接入、不安全终端不联网”,需构建“身份认证-安全检测-动态授权”三位一体的准入控制机制。在身份认证方面,针对不同类型的终端设备采用差异化的身份认证方式,确保终端身份的唯一性与真实性。对于移动医疗终端(如移动医生工作站、护理终端),采用“设备指纹+用户账号密码+多因素认证”的复合认证方式,设备指纹用于识别终端硬件身份,用户账号密码用于验证操作人员身份,多因素认证(如短信验证码、动态口令令牌、生物识别)用于提升认证安全性,防止账号密码被盗用;对于医疗物联网设备(如温湿度传感器、智能输液泵),采用“数字证书+设备唯一标识”的认证方式,为每台物联网设备颁发唯一的数字证书与设备标识,通过证书验证实现设备身份的自动认证,避免未授权物联网设备接入网络;对于远程医疗设备(如远程手术机器人、高清会诊终端),采用“VPN加密接入+多因素认证”的方式,远程设备需先通过VPN接入医院内部网络,再进行身份认证,确保远程接入链路的安全与终端身份的可靠。^①

在安全检测方面,终端接入网络前需通过终端安全管理平台进行全面的安全状态检测,检测内容包括终端操作系统版本、安全补丁更新情况、杀毒软件安装与病毒库更新状态、终端防火墙配置、敏感数据加密存储情况、是否存在恶意软件等。对于移动医疗终端,还需检测终端是否Root/越狱、是否安装未授权应用程序、是否开启加密存储功能等;对于医疗物联网设备,需检测设备固件版本、是否存在已知漏洞、通信协议是否安全等。安全检测不通过的终端,将被拒绝接入网络,或被隔离至 quarantine 区域进行修复,修复完成并通过安全检测后才能接入网络。在动态授权方面,基于终端的身份类型、安全状态、所属业务部门等信息,通过动态授权机制为终端分配差异化的网络访问权限,实现“最小权限原则”。例如,移动医生工作站仅能访问 HIS 系统、电子病历系统等与其业务相关的核心业务系统,无法访问与业务无关的网络资源;温湿度传感器仅能与边缘节点进行数据通信,无法访问核心业务网络;远程医疗设备仅能访问远程会诊平台、PACS 系统等相关应用系统,且访问权限仅在业务开展期间有效,业务结束后自动回收。

^① 刘谦,孙婷婷.基于VPN技术的区域性远程医疗系统的构想[J].医疗设备信息,2007,(12):43-45.

（二）移动医疗终端安全防护

移动医疗终端具有移动性强、使用场景复杂、数据交互频繁等特点，其安全防护需兼顾安全性与易用性，重点从设备安全、数据安全、应用安全三个维度开展。在设备安全方面，需对移动医疗终端进行安全加固，包括操作系统加固与硬件安全防护。操作系统加固方面，采用定制化的安全操作系统，关闭不必要的系统服务与端口，禁用 USB 调试、蓝牙等不必要的功能，及时推送安全补丁更新，修复系统漏洞；对于 Android 系统终端，需开启 SELinux 安全机制，限制应用程序的权限范围；对于 iOS 系统终端，需开启设备加密功能，设置严格的屏幕解锁密码。硬件安全防护方面，为移动医疗终端配备安全存储芯片，用于存储加密密钥、数字证书等敏感信息，防止密钥泄露；采用防拆设计，当终端被非法拆卸时，自动清除终端内的敏感数据，避免数据泄露。

在数据安全方面，实现移动医疗终端数据的全生命周期加密保护。数据存储加密方面，终端内存储的患者诊疗数据、账号密码等敏感信息需采用 AES-256 等高强度加密算法进行加密存储，加密密钥由终端安全管理平台统一管理，定期更换；对于离线存储的数据，需设置访问密码与加密保护，防止终端丢失或被盗后数据泄露。数据传输加密方面，移动医疗终端与医疗通信网络之间的所有数据传输均采用 SSL/TLS 加密协议，确保数据在传输过程中不被拦截、窃取或篡改；对于远程传输的敏感数据，还需通过 VPN 隧道进行二次加密，进一步提升传输安全性。数据销毁安全方面，建立移动医疗终端数据销毁机制，当终端报废、淘汰或丢失时，通过远程指令或物理销毁的方式彻底清除终端内的敏感数据，确保数据无法被恢复。

在应用安全方面，加强对移动医疗终端应用程序的全生命周期管理。应用程序准入方面，建立移动应用白名单制度，仅允许安装经过安全检测与认证的正规应用程序，禁止安装未授权的第三方应用；医院内部开发的移动应用需进行严格的安全测试，修复已知漏洞后才能部署使用。应用程序权限管理方面，采用精细化的权限管控策略，根据应用程序的业务需求分配最小必要的权限，禁止应用程序获取与其业务无关的权限（如位置信息、通讯录、摄像头等）；定期对应用程序的权限使用情况进行审计，发现违规权限使用行为及时处置。应用程序安全监测方面，通过终端安全管理平台实时监测应用程序的运行状态，及时发现并处置应用程序的异常行为（如恶意收集数据、异常数据传输等）；定期对应用程序进

行漏洞扫描与安全更新,修复潜在安全隐患。

(三) 医疗物联网设备安全防护

医疗物联网设备数量庞大、类型多样、资源受限,其安全防护需采用“轻量化、易部署、低功耗”的防护方案,重点解决固件漏洞、默认凭证、通信安全等核心安全问题。在固件安全防护方面,建立医疗物联网设备固件全生命周期安全管理机制。固件开发阶段,引入安全开发生命周期(SDL)理念,在固件设计、编码、测试等环节融入安全要求,开展漏洞扫描、渗透测试等安全检测,修复已知漏洞;固件发布阶段,采用数字签名技术对固件进行签名,确保固件的完整性与真实性,防止固件被篡改;固件更新阶段,通过加密通道推送固件更新包,终端设备验证固件签名后才能进行更新,避免恶意固件被植入;同时,建立固件漏洞应急响应机制,及时发现并修复已部署设备的固件漏洞,通过远程更新或本地升级的方式推送安全补丁。

在凭证安全防护方面,严格管理医疗物联网设备的默认凭证,杜绝默认凭证滥用问题。设备出厂前,为每台设备设置唯一的默认管理员账号密码,并在设备手册中明确告知用户需及时修改默认凭证;设备部署阶段,强制要求用户修改默认凭证,设置复杂度高、长度足够的密码,并定期更换;对于不支持修改默认凭证的老旧设备,通过网络隔离、访问控制等技术手段限制其访问范围,或逐步淘汰替换。同时,建立设备凭证管理平台,对设备凭证进行集中管理,实现凭证的生成、分发、更换、吊销等全生命周期管理,避免凭证泄露或滥用。

在通信安全防护方面,保障医疗物联网设备与边缘节点、云端平台之间的通信安全。采用安全的通信协议,替代传统的明文传输协议,如将MQTT协议升级为MQTT-SN(基于DTLS加密),将CoAP协议升级为CoAPs(基于DTLS加密),确保数据传输过程中的加密保护;对于LoRa、NB-IoT等物联网通信技术,采用端到端加密方式,加密密钥由医院自主管理,避免依赖运营商的加密机制。同时,在物联网通信网络中部署网络流量分析设备,实时监测设备通信流量的异常情况(如流量突变、异常通信地址、异常数据格式等),及时发现并拦截恶意通信行为;建立物联网设备通信白名单,仅允许设备与授权的服务器或节点进行通信,禁止与未授权地址进行数据交互。

(四) 远程医疗设备安全防护

远程医疗设备直接关系到患者生命安全,其安全防护需重点保障实时控制安

全、数据传输安全与设备协同安全，采用“专用网络+多重加密+实时监测”的防护方案。在专用网络防护方面，为远程医疗设备构建独立的专用通信网络，与医院其他网络进行隔离，避免网络攻击从其他网络渗透至远程医疗设备网络。采用 5G 网络切片技术，为远程医疗业务划分独立的网络切片，确保网络资源的专属使用与隔离防护；切片内部采用加密传输、访问控制等技术手段，防止切片内攻击与切片间渗透；同时，部署切片安全管理平台，实时监测切片网络的运行状态与安全事件，确保切片网络的稳定与安全。

在实时控制安全防护方面，保障远程医疗设备控制指令的安全传输与准确执行。采用低延迟、高可靠的加密传输协议，确保控制指令的实时性与完整性；在控制指令传输过程中，加入校验码与时间戳，防止指令被篡改、重放攻击；部署实时控制安全监测系统，实时监测控制指令的传输延迟、执行状态，当出现延迟超标、指令异常等情况时，立即发出告警，并自动采取应急措施（如暂停远程控制、切换至本地控制模式）。同时，对远程医疗设备的控制权限进行严格管理，采用多因素认证与精细化权限分配机制，仅允许具备资质的医护人员在授权范围内进行远程控制操作；建立控制操作日志审计机制，记录所有控制操作的人员、时间、内容等信息，确保操作可追溯。

在设备协同安全防护方面，保障远程医疗设备与院内其他系统（如 PACS 系统、电子病历系统）之间的协同工作安全。采用标准化的安全接口协议，实现设备与系统之间的安全对接；在接口处部署 API 网关，对接口访问进行身份认证、权限控制、流量限制等，防止接口被滥用与攻击；建立接口数据传输加密机制，确保协同数据的传输安全；定期对接口进行安全测试与漏洞扫描，修复接口安全隐患。同时，建立远程医疗设备协同工作安全监测机制，实时监测设备与系统之间的协同数据传输状态，当出现数据传输异常、格式错误等情况时，立即中断协同连接，避免错误数据影响诊疗业务。

三、网络边界安全防护策略

（一）外部网络边界防护

外部网络边界是医疗通信网络与外部网络（如互联网、运营商网络、跨机构协作网络）的连接点，是抵御外部攻击的关键防线，需构建“多层次、立体化”的边界防护体系。在边界访问控制方面，部署下一代防火墙（NGFW）作为核心

边界防护设备,实现对边界流量的精准识别与访问控制。基于医疗业务需求,制定精细化的访问控制策略,明确允许接入的外部地址、端口、协议等,禁止一切未经授权的外部访问;采用应用识别技术,精准识别网络流量中的应用类型,对不同应用采取差异化的防护策略,如允许远程医疗协作应用的流量通过,禁止娱乐、购物等无关应用的流量接入;同时,开启防火墙的智能防御功能,自动识别与拦截恶意流量、攻击行为。

在恶意流量拦截方面,部署入侵防御系统(IPS)与分布式拒绝服务(DDoS)防护设备,抵御各类网络攻击。IPS设备实时监测边界网络流量,基于特征库与行为分析技术,精准识别并拦截SQL注入、XSS跨站脚本、缓冲区溢出等常见网络攻击;定期更新攻击特征库,提升对新型攻击的识别能力;开启IPS的联动防御功能,与防火墙、安全感知中心等设备协同工作,实现攻击的精准阻断与溯源。DDoS防护设备采用“云端清洗+本地防护”的协同防护方案,云端清洗设备负责对大流量DDoS攻击进行初步清洗,过滤大部分恶意流量;本地防护设备负责对剩余流量进行精细化检测与拦截,确保核心业务不受影响;同时,建立DDoS攻击应急响应机制,当遭遇大规模DDoS攻击时,及时启动流量牵引、带宽扩容等应急措施,保障网络的可用性。

在VPN加密接入防护方面,保障外部授权用户(如远程医护人员、跨机构协作人员)的安全接入。部署企业级VPN网关,支持IPSec、SSL等多种VPN协议,满足不同用户的接入需求;采用高强度的加密算法(如AES-256、RSA-2048)对VPN传输链路进行加密,确保数据传输安全;对VPN接入用户进行严格的身份认证,采用“账号密码+数字证书+多因素认证”的复合认证方式,防止未授权用户接入;精细化分配VPN接入权限,根据用户的身份与业务需求,为其分配最小必要的网络访问权限;建立VPN接入日志审计机制,记录用户接入时间、IP地址、访问资源等信息,确保接入行为可追溯。

(二) 内部网络边界防护

内部网络边界是医疗通信网络内部不同业务区域(如核心业务区、办公区、物联网区、远程医疗区)之间的连接点,需通过网络隔离与访问控制,防止内部攻击的扩散与蔓延。在网络区域划分方面,基于“最小权限原则”与“业务相关性原则”,将医疗通信网络划分为不同的安全区域,如核心业务区(部署HIS、LIS、PACS等核心系统)、办公区(部署办公终端与系统)、物联网区(连接

医疗物联网设备）、远程医疗区（部署远程医疗设备与平台）、DMZ 区（部署对外提供服务的服务器）等。各区域之间通过防火墙、网络隔离设备等实现逻辑隔离，明确各区域之间的通信规则，禁止不同区域之间的非法数据交互。

在区域间访问控制方面，部署内部防火墙或访问控制列表（ACL），实现对不同区域之间流量的精准控制。根据业务需求制定区域间访问控制策略，仅允许必要的业务流量在区域间传输，如核心业务区与办公区之间仅允许办公终端访问核心业务系统的特定端口与服务，禁止核心业务区向办公区的主动数据传输；物联网区仅允许与边缘节点、云端平台之间的通信，禁止直接访问核心业务区；远程医疗区与核心业务区之间仅允许特定协同数据的传输，禁止无关流量交互。同时，采用网络流量分析技术，实时监测区域间的流量状态，及时发现并处置异常流量与违规访问行为。

在敏感区域防护方面，针对核心业务区、数据中心等敏感区域，实施强化防护措施。部署网络隔离设备（如网闸）实现敏感区域与其他区域的物理隔离或空气隔离，确保敏感区域的绝对安全；在敏感区域入口部署 Web 应用防火墙（WAF），防护核心业务系统的 Web 应用安全，拦截针对 Web 应用的攻击（如 SQL 注入、XSS 跨站脚本、恶意爬虫等）；部署数据库审计系统，实时监测核心业务数据库的访问行为，及时发现并处置数据库入侵、数据篡改、数据泄露等安全事件；对敏感区域的网络设备与服务器进行安全加固，关闭不必要的服务与端口，及时更新安全补丁，提升设备自身安全防护能力。

（三）跨机构协作边界防护

跨机构协作边界是医疗通信网络与其他医疗机构、医保部门、科研机构等外部协作单位网络之间的连接点，需在保障协作业务顺利开展的同时，确保医疗通信网络的安全。在协作网络接入方面，采用“专用链路+加密传输”的方式，构建安全的跨机构协作通信链路。优先采用专线（如光纤专线、MSTP 专线）实现跨机构连接，避免使用公共网络传输协作数据；对专线传输链路进行加密保护，采用 AES-256 等高强度加密算法，确保数据传输安全；部署专线安全监测设备，实时监测专线链路的运行状态与数据传输情况，及时发现并处置链路中断、数据泄露等安全事件。

在协作身份认证与授权方面，建立跨机构统一身份认证体系，实现对协作单位用户的身份统一管理 with 认证。采用基于公钥基础设施（PKI）的数字证书认证

方式,为协作单位用户颁发统一的数字证书,通过证书验证实现用户身份的精准识别;采用多因素认证机制,提升身份认证的安全性;建立精细化的权限分配机制,根据协作业务需求,为协作单位用户分配最小必要的网络访问权限与数据使用权限,确保用户仅能访问与协作业务相关的资源,无法访问医院内部敏感数据与核心业务系统。

在协作数据安全防护方面,加强对跨机构协作数据的全流程安全管理。协作数据传输前,对敏感数据进行脱敏处理,去除患者身份信息、诊疗细节等核心敏感内容,仅保留协作所需的必要信息;数据传输过程中,采用加密传输协议,确保数据传输安全;数据接收后,对数据进行安全存储与访问控制,禁止协作单位用户将接收的数据用于协作业务之外的其他用途;建立协作数据使用日志审计机制,记录数据的接收、存储、使用、销毁等全流程信息,确保数据使用可追溯。同时,与协作单位签订安全协议,明确双方的安全责任与义务,规范协作数据的传输与使用行为;定期对协作单位的安全防护能力进行评估,督促协作单位落实安全防护措施,降低协作过程中的安全风险。

四、核心网络安全防护策略

(一) 5G 核心网络安全防护

5G 核心网络是医疗 5G 通信的核心枢纽,其安全直接影响整个 5G 医疗通信网络的安全,需针对 5G 核心网络的虚拟化、软件化特性,从网络功能安全、信令安全、数据安全三个维度开展防护。在网络功能安全防护方面,保障 5G 核心网网络功能实体(如 AMF、SMF、UPF)的安全运行。采用虚拟化安全加固技术,对网络功能虚拟化(NFV)基础设施进行安全加固,关闭不必要的服务与端口,及时更新虚拟化层安全补丁,防止虚拟化层漏洞被利用;部署容器安全管理平台,对网络功能实体的容器化部署进行安全管理,实现容器镜像的安全检测、容器运行状态的实时监测、容器间的隔离防护,防止容器被攻击与逃逸;建立网络功能实体安全监测机制,实时监测实体的运行状态、资源占用情况,及时发现并处置实体异常行为与攻击事件。

在信令安全防护方面,保障 5G 核心网信令的安全传输与处理。采用加密传输协议对信令消息进行加密保护,防止信令消息被拦截、窃取或篡改;部署信令安全监测系统,基于信令特征库与行为分析技术,实时监测信令消息的传输状

态与内容，及时识别并拦截恶意信令攻击（如伪基站攻击、信令风暴攻击、位置劫持攻击等）；对信令接口进行安全加固，实施严格的身份认证与访问控制，防止未经授权设备接入信令网络；定期更新信令安全策略与特征库，提升对新型信令攻击的识别与防护能力。

在数据安全防护方面，保障 5G 核心网络中传输与处理的医疗数据安全。采用端到端加密技术，对医疗数据在 5G 核心网络中的传输过程进行全程加密保护，确保数据传输安全；在数据处理过程中，采用数据隔离与访问控制技术，防止不同用户、不同业务的数据相互泄露；部署数据安全监测系统，实时监测核心网络中医疗数据的传输、处理、存储状态，及时发现并处置数据泄露、篡改等安全事件；建立数据安全审计机制，记录数据的全流程处理信息，确保数据处理行为可追溯。同时，加强 5G 核心网络与传统网络互联互通接口的安全防护，部署接口安全网关，实现接口访问的身份认证、权限控制、流量限制等功能，防止攻击者通过接口从传统网络入侵 5G 核心网络。

（二）WiFi 6 网络安全防护

WiFi 6 网络广泛应用于院内移动办公与患者服务场景，其安全防护需解决传统 WiFi 网络的安全隐患，同时应对 WiFi 6 技术带来的新安全风险，重点从加密机制、接入点安全、漫游安全三个维度开展防护。在加密机制防护方面，采用安全的 WiFi 加密协议，杜绝加密漏洞被利用。强制启用 WiFi 6 推荐的 WPA3 加密协议，替代过时的 WEP、WPA、WPA2 加密协议；WPA3 加密协议采用更强的密钥协商机制与加密算法，提升加密安全性，防止密钥被破解与中间人攻击；对于必须兼容老旧终端的场景，采用 WPA3 与 WPA2 混合模式，并对老旧终端进行严格的身份认证与访问控制，限制其访问范围。同时，加强 WiFi 加密密钥的管理，采用动态密钥生成与定期更换机制，避免密钥长期使用导致泄露；禁止使用弱密钥，通过 WiFi 管理平台强制用户设置复杂度高、长度足够的密钥。

在接入点（AP）安全防护方面，保障 WiFi 6 AP 的安全运行。对 AP 进行安全加固，关闭不必要的服务与端口，及时更新 AP 固件与安全补丁，修复已知漏洞；采用强密码认证机制管理 AP 的管理员账号，禁止使用默认凭证，定期更换管理员密码；部署 AP 安全管理平台，实时监测 AP 的运行状态、接入终端数量、流量情况等，及时发现并处置 AP 异常行为（如非法接入、流量异常、固件篡改等）。同时，严格管控医院内部 AP 的部署，禁止私接 AP 行为；建立 AP 准入登记制度，

所有 AP 均需经过安全检测与登记备案后才能部署使用;定期对院内 AP 进行排查,发现私接 AP 立即拆除,并对相关责任人进行处罚。

在漫游安全防护方面,保障 WiFi 6 终端在不同 AP 之间漫游的安全与流畅。采用 802.11r/k/v 漫游协议,优化漫游切换流程,减少漫游切换时间,降低漫游过程中的安全风险;在漫游切换过程中,保持加密传输的连续性,避免数据传输中断或加密失效;部署漫游安全监测系统,实时监测终端漫游切换状态,及时发现并处置漫游过程中的身份认证异常、数据传输中断等问题。同时,加强漫游过程中的身份认证管理,采用快速重认证机制,确保终端在漫游切换时能够快速完成身份认证,且认证过程安全可靠;建立漫游日志审计机制,记录终端漫游的时间、AP 切换路径、接入身份等信息,确保漫游行为可追溯。

(三) 光纤骨干网络安全防护

光纤骨干网络是医疗通信网络的核心传输链路,承载着大量核心医疗业务数据的传输,其安全防护需重点保障链路的可用性、传输的安全性与数据的完整性。在链路可用性防护方面,构建冗余备份的光纤骨干网络架构,避免单点故障导致链路中断。采用双链路、双路由的冗余设计,核心业务区域之间部署多条光纤链路,当主链路出现故障时,自动切换至备用链路,确保业务连续性;定期对光纤链路进行巡检与维护,检查链路的传输质量、物理状态,及时发现并修复链路故障(如光纤断裂、接口松动等);部署链路监测系统,实时监测链路的传输速率、延迟、误码率等指标,当出现指标异常时,立即发出告警,通知运维人员及时处置。

在传输安全防护方面,保障光纤骨干网络中数据传输的安全。采用波分复用(WDM)技术与加密传输技术相结合的方式,实现数据的安全传输;在光纤链路两端部署光传输加密设备,采用高强度的加密算法对传输数据进行加密保护,防止数据在传输过程中被拦截、窃取或篡改;加密密钥由安全管理平台统一管理,定期更换,确保密钥安全。同时,加强光纤链路的物理安全防护,对光纤敷设路径进行安全规划,避免敷设在易被破坏、易被监听的区域;对光纤接头、光交箱等设备进行物理隔离与安全防护,设置防盗、防破坏装置,防止设备被非法接触与破坏;建立光纤链路物理安全巡检机制,定期对光纤敷设路径与设备进行巡检,及时发现并处置物理安全隐患。

在数据完整性防护方面,保障光纤骨干网络中传输数据的完整性与准确性。采用数据校验与纠错技术,在数据传输过程中加入校验码,接收端对数据进行校

验,发现数据错误时及时纠错;部署数据完整性监测系统,实时监测传输数据的完整性,当发现数据被篡改时,立即中断数据传输,发出告警,并启动数据恢复机制;建立数据传输日志审计机制,记录数据传输的时间、来源、目的地、数据量等信息,确保数据传输行为可追溯。同时,加强光纤骨干网络设备的安全防护,对核心路由器、交换机等设备进行安全加固,关闭不必要的服务与端口,及时更新安全补丁,设置强密码认证机制,防止设备被攻击与控制。

(四) 多网络融合安全防护

多网络融合是医疗通信网络的发展趋势,“5G+WiFi 6+ 光纤+物联网”的融合架构需解决网络异构性带来的安全风险,实现不同网络的协同安全防护。在融合网络接入控制方面,构建统一的终端准入控制体系,实现对不同网络终端的统一身份认证、安全状态检查与动态授权。通过统一的终端准入平台,对接入5G、WiFi 6、物联网等不同网络的终端进行集中管理,确保只有安全合规的终端才能接入融合网络;基于终端的身份类型、安全状态、所属业务等信息,为终端分配跨网络的统一访问权限,实现终端在不同网络之间的无缝漫游与安全接入。

在融合网络流量调度安全方面,保障数据在不同网络之间的安全流转与调度。部署统一的流量调度平台,基于业务需求、网络状态等因素,实现数据在不同网络之间的智能调度;在流量调度过程中,采用加密传输、完整性校验等技术手段,确保数据流转安全;建立流量调度安全监测机制,实时监测流量调度状态,及时发现并处置流量异常、调度错误等问题。同时,加强融合网络边界的安全防护,在不同网络的融合节点部署安全网关,实现网络之间的隔离防护与安全访问控制;制定统一的网络安全策略,确保不同网络的安全策略协同一致,避免因安全策略差异导致安全漏洞。

在融合网络管理安全方面,构建统一的网络安全管理平台,实现对多网络的集中管理与运营。通过统一的管理平台,实现对5G、WiFi 6、光纤、物联网等不同网络设备的集中监控、配置管理、漏洞管理、安全审计等功能;整合各网络的安全日志、告警信息,通过大数据分析、人工智能检测等技术实现对安全威胁的全局感知与精准识别;建立统一的安全事件应急响应机制,实现不同网络安全事件的协同处置,提升应急响应效率。同时,加强融合网络的安全运维管理,建立跨网络的安全运维团队,明确各团队的安全职责与协作流程;定期开展跨网络的安全演练,提升运维人员的协同防护能力与应急处置能力。

五、算力节点安全防护策略

（一）边缘节点安全防护

边缘节点部署在医院各楼层、门诊楼、住院楼等分散区域，承担着本地医疗数据的实时处理、缓存与转发功能，其安全防护需兼顾安全性与实时性，重点从物理安全、软件安全、数据安全三个维度开展。在物理安全防护方面，保障边缘节点硬件设备的物理安全。为边缘节点部署物理安全防护装置，如防盗机柜、门禁系统、视频监控系统等，防止设备被非法接触、盗窃或破坏；对边缘节点的部署环境进行安全规划，避免部署在易被干扰、易发生自然灾害的区域；建立物理安全巡检机制，定期对边缘节点的物理环境与设备状态进行巡检，及时发现并处置物理安全隐患。

在软件安全防护方面，保障边缘节点软件平台与应用程序的安全运行。对边缘计算平台（如 Kubernetes Edge、EdgeX Foundry）进行安全加固，关闭不必要的服务与端口，及时更新软件补丁，修复已知漏洞；部署容器安全管理工具，对容器化部署的应用程序进行安全管理，实现容器镜像的安全检测、容器运行状态的实时监测、容器间的隔离防护；建立软件安全监测机制，实时监测边缘节点软件平台与应用程序的运行状态，及时发现并处置软件异常行为与攻击事件。同时，加强边缘节点的访问控制，采用强密码认证、多因素认证等机制，严格控制边缘节点的访问权限；建立访问日志审计机制，记录所有访问边缘节点的行为，确保访问行为可追溯。

在数据安全防护方面，保障边缘节点缓存与处理的医疗数据安全。采用加密存储技术，对边缘节点缓存的医疗数据进行加密保护，加密密钥由安全管理平台统一管理，定期更换；对数据处理过程中的中间数据进行加密保护，防止数据泄露；部署数据安全监测系统，实时监测边缘节点数据的缓存、处理、传输状态，及时发现并处置数据泄露、篡改等安全事件。同时，建立数据备份与恢复机制，定期对边缘节点缓存的数据进行备份，备份数据采用加密存储，并存储在安全的位置；当边缘节点数据发生丢失或损坏时，能够快速从备份中恢复数据，保障医疗业务连续性。此外，加强边缘节点与云端平台、终端设备之间数据传输的安全防护，采用加密传输协议，确保数据传输安全。

（二）云端数据中心安全防护

云端数据中心是医疗通信网络的核心数据存储与算力处理中心，汇聚了海量医疗数据，其安全防护需采用“全方位、多层次”的防护方案，重点从存储安全、虚拟化安全、访问控制安全三个维度开展。在存储安全防护方面，保障医疗数据的存储安全与可用性。采用存储加密技术，对云端数据中心存储的医疗数据进行静态加密，加密算法采用 AES-256 等高强度加密算法，加密密钥由密钥管理系统统一管理，实现密钥的安全生成、分发、更换、吊销等全生命周期管理；对存储设备进行安全加固，关闭不必要的服务与端口，及时更新固件与安全补丁，防止存储设备被攻击与控制。

建立多副本备份与异地容灾备份机制，确保数据的可用性与完整性。核心医疗数据采用多副本存储，在同一数据中心内存储多个数据副本，当某一副本损坏时，可快速切换至其他副本；同时，在异地部署容灾备份中心，定期将核心医疗数据备份至容灾中心，容灾中心采用与主数据中心相同的安全防护标准，确保备份数据的安全；建立数据备份与恢复测试机制，定期对备份数据进行恢复测试，确保备份数据的可用性与恢复效率。此外，部署存储安全监测系统，实时监测存储设备的运行状态、数据存储状态，及时发现并处置存储设备故障、数据损坏、数据泄露等安全事件。

在虚拟化安全防护方面，保障云端数据中心虚拟化环境的安全运行。对虚拟化平台（如 VMware、KVM）进行安全加固，关闭不必要的服务与端口，及时更新虚拟化层安全补丁，修复虚拟化层漏洞；部署虚拟化安全管理平台，实现对虚拟机的全生命周期管理，包括虚拟机的创建、部署、运行、销毁等环节的安全管控；加强虚拟机之间的隔离防护，采用虚拟防火墙、VLAN 隔离等技术手段，防止虚拟机之间的攻击与数据泄露；对虚拟机镜像进行安全管理，实现镜像的安全检测、加密存储、版本控制等，防止恶意镜像被部署使用。

在访问控制安全防护方面，保障云端数据中心的访问安全。采用精细化的访问控制策略，基于用户的身份、角色、业务需求等信息，为用户分配最小必要的访问权限；采用多因素认证机制，提升用户身份认证的安全性，防止账号密码被盗用；部署访问控制服务器，实现对用户访问行为的集中控制与管理；建立访问日志审计机制，记录所有用户访问云端数据中心的行为，包括访问时间、访问 IP、访问资源、操作内容等信息，确保访问行为可追溯。同时，加强云端数据中

心远程访问的安全防护，仅允许通过 VPN 等加密方式进行远程访问；对远程访问用户进行严格的身份认证与权限控制，限制远程访问的时间与范围；部署远程访问安全监测系统，实时监测远程访问行为，及时发现并处置远程访问攻击事件。

六、安全管理与运营策略

（一）安全管理制度体系建设

安全管理制度体系是医疗通信网络安全防护策略有效落地的保障，需构建覆盖“规划、建设、运维、应急”全生命周期的管理制度体系。在规划阶段，制定《医疗通信网络安全规划管理办法》，明确安全规划的原则、目标、流程与职责，确保安全防护与网络建设同步规划、同步设计；制定《医疗通信网络安全需求分析规范》，明确不同业务场景的安全需求，为安全防护方案的设计提供依据。在建设阶段，制定《医疗通信网络安全建设管理办法》，规范安全设备的选型、采购、部署流程，确保安全设备符合安全需求与行业标准；制定《医疗通信网络安全集成规范》，规范安全系统的集成流程与技术要求，确保安全系统与现有网络、业务系统的无缝对接。

在运维阶段，制定《医疗通信网络安全运维管理办法》，规范日常安全运维流程，包括安全设备监控、漏洞管理、补丁更新、日志审计等；制定《终端安全管理规范》《网络设备安全管理规范》《数据安全管理制度》等专项管理制度，明确不同类型设备与数据的安全管理要求；制定《安全事件报告与处置流程》，规范安全事件的发现、报告、处置、总结等流程，确保安全事件能够快速响应、有效处置。在应急阶段，制定《医疗通信网络安全应急预案》，明确应急组织架构、应急响应流程、应急处置措施等，针对不同类型的安全事件（如 DDoS 攻击、数据泄露、网络中断等）制定专项应急处置方案；建立应急演练机制，定期开展安全应急演练，提升应急处置能力与协同配合能力。

同时，加强安全管理制度的宣贯与培训，确保医院内部各部门、各岗位人员熟悉并严格遵守安全管理制度；建立安全管理制度评审与更新机制，定期对管理制度进行评审，根据法律法规更新、技术发展变化、业务需求调整等情况及时修订完善管理制度，确保管理制度的时效性与适用性。

（二）安全运营团队建设

安全运营团队是医疗通信网络安全防护的执行主体，需打造一支“专业能力

强、协作效率高”的安全运营团队。在团队组建方面，根据医疗通信网络的规模与安全需求，配备足够数量的安全专业人员，包括安全架构师、安全运维工程师、安全检测工程师、应急响应工程师等；明确各岗位的职责与分工，确保安全运营工作的有序开展。安全架构师负责安全防护体系的规划、设计与优化；安全运维工程师负责安全设备的日常运维、漏洞管理、补丁更新等；安全检测工程师负责安全威胁的实时监测、漏洞扫描、渗透测试等；应急响应工程师负责安全事件的应急处置、调查分析、溯源追踪等。

在能力提升方面，建立常态化的安全培训与学习机制，提升团队成员的专业能力。定期组织内部培训，邀请内部技术骨干或外部安全专家开展安全技术、安全策略、应急处置等方面的培训；鼓励团队成员参加外部专业培训与认证（如 CISSP、CISP、CEH 等），提升专业资质与技术水平；建立知识共享平台，促进团队成员之间的技术交流与知识共享；定期开展安全技术研讨，针对新型安全威胁、技术发展趋势等进行深入分析，提升团队的技术前瞻性与应对能力。

在协作机制方面，建立安全运营团队与医院内部其他部门（如信息科、医务科、后勤科、临床科室等）的协同协作机制。明确各部门在安全管理工作中的职责与协作流程，加强信息共享与沟通协调；定期召开安全工作协调会议，通报安全运营情况，解决安全管理工作中遇到的问题；建立跨部门的安全应急响应团队，确保安全事件发生时能够快速协同处置。同时，加强与外部安全服务商、运营商、行业协会等的合作，借助外部专业力量提升安全运营能力；建立外部安全专家智库，为复杂安全问题的解决提供技术支持。

（三）安全监测与应急响应体系建设

安全监测与应急响应体系是及时发现并处置安全威胁的关键，需构建“实时监测、精准预警、快速响应、有效处置”的全流程体系。在安全监测方面，构建统一的安全感知中心，整合各防护域的安全监测设备（如防火墙、IPS、WAF、流量分析系统、终端安全管理平台等）的日志与告警信息，实现对安全威胁的集中监测与统一管理。采用大数据分析、人工智能检测等技术，对海量安全数据进行深度分析，实现对新型安全威胁的精准识别与预警；建立安全威胁情报共享机制，及时获取外部安全威胁情报（如新型漏洞、攻击手段等），并融入安全监测系统，提升威胁识别能力。

针对不同类型的安全威胁，建立专项监测机制。网络攻击监测方面，实时监

测网络流量中的恶意行为，如 DDoS 攻击、SQL 注入、XSS 跨站脚本等，及时发出告警并采取拦截措施；数据泄露监测方面，实时监测医疗数据的传输、存储、使用状态，及时发现并处置数据泄露行为；终端安全监测方面，实时监测终端设备的安全状态，如漏洞情况、恶意软件感染情况等，督促终端及时修复安全隐患；应用安全监测方面，实时监测 Web 应用、API 接口的运行状态，及时发现并处置应用漏洞与攻击行为。

在应急响应方面，建立完善的应急响应机制，确保安全事件能够快速、有效处置。建立应急响应组织架构，明确应急指挥小组、技术处置小组、协调保障小组等各小组的职责与分工；制定详细的应急响应流程，包括事件发现与报告、事件分析与评估、应急处置、事件总结与改进等环节；针对不同类型的安全事件，制定专项应急处置方案，明确处置步骤、技术措施、责任人员等。建立应急响应资源保障机制，配备必要的应急设备、技术工具、备份数据等，确保应急处置工作的顺利开展；定期开展应急演练，模拟不同类型的安全事件，检验应急响应机制的有效性 with 团队的应急处置能力，及时发现并改进应急响应工作中的问题。

同时，建立安全事件追溯与总结机制，对每起安全事件的原因、处置过程、造成的影响等进行深入分析，总结经验教训，优化安全防护策略与应急响应机制；建立安全事件通报与上报机制，及时向医院管理层、相关监管部门通报安全事件情况，确保信息透明与合规上报。

（四）安全审计与合规管理

安全审计与合规管理是确保医疗通信网络安全防护策略符合法律法规与行业标准的重要保障，需构建“全流程、全覆盖”的安全审计与合规管理体系。在安全审计方面，建立统一的安全审计平台，实现对医疗通信网络中所有安全相关行为的全程审计。审计范围覆盖终端接入、网络传输、算力节点、应用服务等全链路，审计内容包括用户访问行为、网络流量行为、数据操作行为、设备运行行为等；采用自动化审计工具，实现审计数据的实时采集、分析与存储，提升审计效率；建立审计日志管理机制，确保审计日志的完整性、真实性与可追溯性，审计日志保存时间符合相关法律法规要求。

针对不同类型的审计对象，制定专项审计方案。用户访问审计方面，审计用户登录、权限变更、数据访问等行为，及时发现并处置违规访问行为；网络流量审计方面，审计网络流量的来源、目的地、传输内容等，及时发现并处置异常流

量与攻击行为；数据操作审计方面，审计医疗数据的创建、修改、删除、导出等行为，确保数据操作合规；设备运行审计方面，审计网络设备、安全设备、服务器等设备的配置变更、固件更新、故障处理等行为，确保设备运行安全。定期开展专项安全审计与全面安全审计，专项审计针对特定安全问题或业务场景开展，全面审计覆盖整个医疗通信网络的安全状况；审计完成后，生成审计报告，提出整改建议，督促相关部门落实整改措施。

在合规管理方面，建立合规性评估与管理机制，确保医疗通信网络安全防护工作符合相关法律法规与行业标准。定期开展合规性评估，对照《网络安全法》《数据安全法》《个人信息保护法》《医疗卫生机构网络安全管理办法》等法律法规与行业标准，对医疗通信网络的安全防护策略、管理制度、技术措施等进行全面评估，识别合规性风险；建立合规性风险台账，明确风险点、整改措施、责任人员与整改期限，督促相关部门落实整改，消除合规性风险。

加强合规性培训与宣贯，提升医院内部各部门、各岗位人员的合规意识，确保其了解并遵守相关法律法规与行业标准；建立合规性更新机制，及时跟踪法律法规与行业标准的更新变化，调整安全防护策略与管理制度，确保持续合规。同时，积极配合相关监管部门的监督检查，提供必要的审计日志、合规性评估报告等资料，确保监管检查顺利通过。

第三节 数据隐私保护与合规管理

一、医疗数据隐私保护体系构建

（一）体系构建核心目标与原则

医疗数据隐私保护体系构建的核心目标是实现医疗数据全生命周期的安全可控，防范数据泄露、篡改、滥用等风险，保障患者的隐私权与数据主权，同时支撑医疗业务的合法合规开展。围绕这一核心目标，体系构建需遵循“以患者为中心、全生命周期防护、分级分类施策、技术与管理并重、协同联动保障”五大核心原则。以患者为中心原则要求将患者数据隐私保护需求贯穿体系构建全流程，明确患者对其数据的知情权、访问权、更正权、删除权等权利，建立便捷的权利行使机制，确保患者数据权益得到有效保障。

全生命周期防护原则强调覆盖医疗数据从产生、采集、传输、存储、使用、共享、销毁到归档的全流程，针对不同环节的安全风险制定差异化的防护措施，形成闭环管理。分级分类施策原则基于医疗数据的敏感程度、重要性及业务需求，对数据进行科学分级分类，对高敏感数据（如患者身份信息、基因数据、诊疗记录核心信息）实施高强度防护，对一般数据实施精准化防护，提升防护资源利用效率。技术与管理并重原则要求既要部署先进的技术防护手段，又要建立完善的管理制度与流程，通过技术赋能管理、管理规范技术应用，实现技术与管理的协同增效。协同联动原则强调医院内部各部门（信息科、医务科、质控科、法务科等）之间的协同配合，以及与监管部门、行业协会、安全服务商等外部机构的联动协作，形成全方位的隐私保护合力。

（二）体系核心架构与功能模块

医疗数据隐私保护体系以“数据安全治理中心”为核心，构建“数据分级分类管理域、全生命周期防护域、安全技术支撑域、管理规范保障域、应急响应处置域”五大核心架构，各架构相互关联、协同运行，实现对医疗数据隐私的全方位保护。数据安全治理中心作为体系的“中枢”，负责统筹规划隐私保护策略，协调各域资源，开展数据安全风险评估与合规性检查，推动隐私保护措施落地执行与持续优化。

数据分级分类管理域是体系的基础支撑模块，核心功能包括数据资产梳理、分级分类标准制定、数据标签管理、分级分类动态更新等。通过数据资产梳理，全面掌握医院医疗数据的种类、数量、存储位置、流转路径、关联业务等信息，建立完整的数据资产台账；依据相关法律法规与行业标准，结合医院业务实际，制定科学的分级分类标准，将医疗数据划分为极高敏感、高敏感、中敏感、低敏感四个等级，明确不同等级数据的界定范围与防护要求；为各类数据打上唯一的数据标签，标签包含数据等级、所属业务、产生时间、责任人等信息，实现数据的精准识别与追溯；建立分级分类动态更新机制，根据业务发展、数据用途变化及法律法规更新，及时调整数据分级分类结果。

全生命周期防护域是体系的核心执行模块，按数据流转环节划分为数据采集防护、传输防护、存储防护、使用防护、共享防护、销毁防护七个子模块。数据采集防护模块负责规范数据采集行为，确保采集过程合法合规，采集数据真实准确，避免过度采集；传输防护模块保障数据在不同系统、不同机构之间传输过程

中的安全，防止数据被拦截、窃取或篡改；存储防护模块实现数据存储过程中的加密保护、访问控制、备份恢复等功能；使用防护模块规范数据使用行为，防止数据滥用与非法访问；共享防护模块管控数据跨机构、跨部门共享过程中的安全，确保共享数据安全可控；销毁防护模块确保数据在达到保存期限或不再使用时，能够彻底、安全地销毁，防止数据残留与泄露。

安全技术支撑域为体系提供技术保障，核心功能模块包括数据加密技术平台、访问控制管理系统、数据脱敏系统、数据泄露检测系统、安全审计系统等。数据加密技术平台采用对称加密、非对称加密、同态加密等多种加密技术，实现数据在传输、存储、使用等环节的加密保护；访问控制管理系统基于角色的访问控制（RBAC）、基于属性的访问控制（ABAC）等技术，实现对数据访问权限的精细化管控；数据脱敏系统通过静态脱敏、动态脱敏等技术，对敏感数据进行处理，确保数据在非生产环境或共享场景下的安全使用；数据泄露检测系统通过流量分析、行为分析等技术，实时监测数据泄露行为，及时发出告警；安全审计系统对数据全生命周期的操作行为进行全程审计，确保操作可追溯。

管理规范保障域为体系提供制度与组织保障，核心功能包括管理制度体系建设、组织架构搭建、人员培训与考核、第三方服务机构管理等。建立覆盖数据隐私保护全流程的管理制度体系，明确各部门、各岗位的职责与分工；搭建专门的数据安全治理组织架构，配备专业的 data security 人员，负责数据隐私保护工作的统筹协调与日常管理；定期开展数据隐私保护培训与考核，提升医院内部人员的隐私保护意识与专业能力；加强对第三方服务机构（如云服务商、软件供应商、科研协作机构）的管理，明确双方的隐私保护责任与义务，确保第三方机构合规使用医疗数据。

应急响应处置域负责应对数据隐私安全事件，核心功能包括应急预案制定、应急响应机制建立、事件调查与处置、事后总结与改进等。制定针对性的医疗数据隐私安全应急预案，明确应急组织架构、响应流程、处置措施等；建立快速响应机制，确保在发生数据泄露、篡改等隐私安全事件时，能够及时启动应急响应，快速处置，降低事件造成的影响；对隐私安全事件进行深入调查，追溯事件原因，明确责任主体；及时总结事件处置经验教训，优化隐私保护体系与应急响应机制。

（三）与现有信息化体系的融合适配

医疗数据隐私保护体系的建设需与医院现有信息化体系（如 HIS、LIS、

PACS、电子病历系统、数据中心等)实现深度融合适配,避免形成“防护孤岛”,确保隐私保护措施与业务应用协同发展。在数据层面,需将数据分级分类管理要求嵌入现有数据管理体系,通过接口对接、数据标签关联等方式,实现数据分级分类结果与现有数据资产的同步更新;将数据加密、脱敏等技术手段与现有数据存储、传输系统对接,实现敏感数据的自动加密传输与存储,无需对现有业务系统进行大规模改造。

在应用层面,需将访问控制、安全审计等隐私保护措施与现有医疗业务应用系统无缝衔接,确保在不影响业务正常开展的前提下,实现对数据使用行为的有效管控。例如,在电子病历系统中嵌入访问控制模块,根据医护人员的岗位、职责等信息,自动分配数据访问权限;在 PACS 系统中集成安全审计功能,对医疗影像数据的查看、导出、共享等操作进行全程记录。同时,需充分考虑现有信息化系统的技术架构与性能要求,选择兼容性强、性能损耗小的隐私保护技术与产品,避免因部署隐私保护措施导致系统响应速度下降、业务流程受阻。

在管理层面,需将数据隐私保护管理制度与现有信息化管理制度、医疗业务管理制度相融合,将隐私保护要求嵌入到信息化项目建设、运维管理、业务操作等全流程。例如,在信息化项目立项阶段,增加数据隐私保护需求评估环节;在项目验收阶段,将隐私保护措施的落实情况作为重要验收指标;在日常运维管理中,将数据安全漏洞修复、隐私保护措施巡检纳入运维流程;在业务操作中,明确医护人员、行政人员等不同岗位的隐私保护操作规范。此外,需推动现有信息化系统的升级改造,提升系统的隐私保护能力,例如对老旧系统进行安全加固,完善系统的数据访问控制、日志审计等功能,确保系统符合隐私保护相关要求。

二、医疗数据全生命周期隐私保护策略

(一) 数据采集环节隐私保护

数据采集是医疗数据全生命周期的起点,其隐私保护的核心是确保采集行为合法合规、数据真实准确、避免过度采集。在采集规范方面,需严格遵循“合法、正当、必要”原则,依据医疗业务需求明确数据采集范围与内容,不得采集与业务无关的个人信息。例如,在患者就诊时,仅采集支撑诊疗服务所需的身份信息、病史信息、检查检验信息等,不得强制采集患者的宗教信仰、收入状况等无关信息。同时,需向患者充分告知数据采集的目的、范围、使用方式、存储期限等信

息,获得患者的明示同意;对于未成年人、精神障碍患者等特殊群体的个人信息,需获得其监护人的同意。

在采集方式方面,需规范数据采集流程,采用安全可靠的采集工具与设备,确保采集数据的真实性与完整性。对于手工录入的数据,需建立数据录入校验机制,对录入数据的格式、准确性进行实时校验,避免因人为操作失误导致数据错误;对于自动采集的数据(如医疗物联网设备采集的生理参数、检验设备采集的检验结果),需对采集设备进行安全认证与加密配置,防止设备被篡改或伪造数据。同时,需建立采集数据的质量管控机制,定期对采集数据进行质量检查,及时清理无效数据、错误数据,确保数据质量。

在身份认证与授权方面,需对数据采集人员进行严格的身份认证与权限控制,确保只有具备相应资质的人员才能开展数据采集工作。采用“账号密码+多因素认证”的复合认证方式,防止采集人员账号被盗用;基于岗位需求为采集人员分配最小必要的采集权限,明确采集人员的操作范围与责任;建立采集人员操作日志审计机制,记录采集人员的身份、采集时间、采集内容、采集方式等信息,确保采集行为可追溯。此外,对于第三方机构参与数据采集的场景(如科研数据采集、体检数据采集),需与第三方机构签订数据采集安全协议,明确双方的责任与义务,对第三方机构的采集行为进行全程监督与管控。

(二) 数据传输环节隐私保护

数据传输环节的隐私保护核心是确保数据在传输过程中不被拦截、窃取、篡改或伪造,需构建“加密传输+链路防护+传输校验”三位一体的防护体系。在加密传输方面,根据数据的敏感等级选择合适的加密方式,实现数据传输的全程加密。对于极高敏感、高敏感数据(如患者基因数据、核心诊疗记录),采用端到端加密方式,使用 AES-256、RSA-2048 等高强度加密算法,确保数据从发送端到接收端全程加密,即使传输链路被攻破,攻击者也无法获取明文数据;对于中敏感、低敏感数据,采用传输层加密方式(如 SSL/TLS 协议),确保数据在传输过程中的安全。同时,需加强加密密钥的管理,采用密钥管理系统实现密钥的安全生成、分发、更换、吊销等全生命周期管理,防止密钥泄露。

在链路防护方面,针对不同的传输链路类型(如内部局域网传输、互联网传输、跨机构专线传输)制定差异化的防护策略。在内部局域网传输中,部署网络防火墙、入侵防御系统等设备,对传输流量进行实时监测与管控,拦截恶意流量与攻击行

为；在互联网传输中，采用 VPN 专线、云安全网关等技术，构建安全的传输通道，避免数据在公共网络中裸传；在跨机构专线传输中，选择安全可靠的专线服务（如光纤专线、MSTP 专线），对专线链路进行加密保护，部署专线安全监测设备，实时监测链路的运行状态与数据传输情况，及时发现并处置链路中断、数据泄露等安全事件。

在传输校验方面，建立数据传输完整性与真实性校验机制，确保数据在传输过程中不被篡改或伪造。在数据传输前，为数据添加唯一的校验码（如 MD5、SHA-256）与时间戳，接收端在收到数据后，通过校验码验证数据的完整性，通过时间戳防止数据被重放攻击；对于重要数据的传输，采用双向认证机制，发送端与接收端相互验证对方的身份，确保数据传输对象的真实性。同时，建立数据传输异常监测机制，实时监测数据传输的速率、流量、延迟等指标，当出现指标异常（如流量突变、延迟超标、数据丢失）时，立即发出告警，通知运维人员及时处置；建立数据传输日志审计机制，记录数据传输的发送端、接收端、传输时间、数据量、加密方式等信息，确保传输行为可追溯。

（三）数据存储环节隐私保护

数据存储环节的隐私保护核心是确保数据存储安全，防止数据被非法访问、篡改、泄露或丢失，需构建“加密存储+访问控制+备份恢复+存储介质管理”全方位的防护体系。在加密存储方面，根据数据的存储方式（如本地存储、云端存储、分布式存储）选择合适的加密技术，实现数据的静态加密保护。对于本地存储的敏感数据，采用存储设备加密、文件系统加密等方式，对存储介质进行整体加密，防止存储介质被盗或丢失后数据泄露；对于云端存储的数据，选择具备合规资质的云服务商，采用云存储加密技术（如服务器端加密、客户端加密），确保数据在云端存储的安全；对于分布式存储的数据，采用分布式加密技术，对数据分片进行加密存储，防止单一节点被攻破导致数据泄露。同时，需定期对加密存储系统进行安全检测与维护，确保加密功能正常运行。

在访问控制方面，建立精细化的存储数据访问控制机制，实现“未授权访问不可行、授权访问可追溯”。基于数据分级分类结果与用户岗位需求，采用 RBAC、ABAC 等访问控制模型，为用户分配最小必要的访问权限，明确用户的访问范围与操作权限；对高敏感数据的访问实施严格的审批流程，用户需提交访问申请，经相关负责人审批通过后才能获得访问权限；采用多因素认证机制，提

升用户身份认证的安全性，防止账号密码被盗用；建立存储数据访问日志审计机制，记录用户的访问身份、访问时间、访问内容、操作行为等信息，及时发现并处置违规访问行为。

在备份恢复方面，建立完善的医疗数据备份与恢复机制，确保数据的可用性与完整性。根据数据的重要性与业务需求，制定差异化的备份策略，核心业务数据采用“实时备份+定时备份+异地容灾备份”的多重备份方式，实时备份确保数据的实时同步，定时备份（如 hourly 级、daily 级）确保数据的定期留存，异地容灾备份确保在主数据中心发生故障时，能够快速从异地容灾中心恢复数据；备份数据采用加密存储方式，确保备份数据的安全；建立备份数据恢复测试机制，定期对备份数据进行恢复测试，检验备份数据的可用性与恢复效率，优化备份与恢复策略。

在存储介质管理方面，加强对存储介质（如硬盘、U 盘、移动硬盘、光盘）的全生命周期管理，防止存储介质滥用导致数据泄露。建立存储介质准入登记制度，所有存储介质均需经过安全检测与登记备案后才能使用；对存储敏感数据的存储介质进行加密处理与专人保管，明确保管责任；建立存储介质使用日志审计机制，记录存储介质的使用人员、使用时间、使用用途、数据读写情况等信息；对于报废、淘汰的存储介质，采用物理销毁（如粉碎、焚烧）或数据彻底清除（如多次覆写、消磁）的方式，确保存储介质中的数据无法被恢复；禁止使用私人存储介质存储医疗数据，防止数据外泄。

（四）数据使用环节隐私保护

数据使用环节的隐私保护核心是规范数据使用行为，防止数据滥用、非法使用，需构建“权限管控+行为监测+数据脱敏”三位一体的防护体系。在权限管控方面，基于数据分级分类结果与业务需求，进一步细化数据使用权限，实现对数据使用的精准管控。例如，医护人员仅能在诊疗过程中使用患者的诊疗数据，且仅能访问与自己负责患者相关的数据；科研人员在使用科研数据时，仅能访问经过脱敏处理的数据集，无法获取患者的真实身份信息；行政人员在使用统计数据时，仅能访问汇总数据，无法访问个体明细数据。同时，建立数据使用权限动态调整机制，根据用户岗位变动、业务需求变化等情况，及时调整用户的使用权限，确保权限与需求匹配。

在行为监测方面，建立实时的医疗数据使用行为监测机制，及时发现并处置

违规使用行为。部署数据使用行为分析系统，通过对用户的操作行为、数据访问频率、数据导出数量、访问时间等维度进行分析，识别异常使用行为（如非工作时间大量访问敏感数据、频繁导出核心诊疗数据、访问与业务无关的数据等）；建立分级告警机制，根据异常行为的严重程度发出不同级别的告警，对于严重违规行为，立即触发应急响应，采取暂停用户权限、阻断数据访问等措施；建立数据使用行为日志审计机制，记录用户的使用行为全流程信息，确保行为可追溯，为违规行为的调查与处理提供依据。

在数据脱敏方面，针对不同的使用场景（如科研、教学、培训、系统测试）采用差异化的脱敏技术，确保敏感数据在使用过程中不泄露患者隐私。在科研数据使用场景中，采用静态脱敏技术，对原始数据进行脱敏处理（如替换、删除、加密、泛化），去除患者的身份标识信息（如姓名、身份证号、联系方式），生成可供科研使用的脱敏数据集，脱敏后的数据集无法关联到具体患者；在系统测试、培训场景中，采用动态脱敏技术，当用户访问测试数据、培训数据时，系统自动对敏感字段进行脱敏处理，用户仅能看到脱敏后的信息，而原始数据仍保持加密存储；对于需要对外展示的医疗数据（如医院官网发布的统计数据），采用数据聚合、匿名化处理等方式，确保数据无法识别到个体患者。同时，建立脱敏数据质量评估机制，确保脱敏后的数据既符合隐私保护要求，又能满足使用需求。

（五）数据共享环节隐私保护

数据共享环节的隐私保护核心是平衡数据共享利用与隐私保护的关系，确保数据共享安全可控，需构建“共享审批+加密传输+访问管控+脱敏处理”全流程的防护体系。在共享审批方面，建立严格的医疗数据共享审批机制，明确共享的条件、流程与责任主体。任何单位或个人需要共享医疗数据时，均需提交共享申请，说明共享目的、共享范围、共享方式、使用期限、接收方资质等信息；医院数据安全治理中心对共享申请进行审核，评估共享行为的合法性、安全性与必要性，对于涉及高敏感数据的共享申请，需经医院管理层审批通过后才能实施；建立共享审批台账，记录共享申请的审核过程、审批结果等信息，确保共享审批可追溯。

在加密传输方面，采用安全可靠的传输方式实现共享数据的加密传输，确保数据在共享过程中的安全。对于跨机构数据共享，优先采用专线传输、VPN加密传输等方式，避免使用公共网络传输共享数据；对于云端共享数据，采用云安

全网关、数据加密传输协议等技术，确保数据在云端传输的安全；无论采用何种传输方式，均需对共享数据进行全程加密，使用高强度加密算法，防止数据被拦截、窃取或篡改。同时，加强对传输链路的安全监测，实时监测传输状态，及时发现并处置传输异常问题。

在访问管控方面，建立共享数据的访问控制机制，确保接收方仅能在授权范围内使用共享数据。与接收方签订数据共享安全协议，明确双方的隐私保护责任与义务，限制接收方的共享数据使用范围与用途，禁止接收方将共享数据用于协议约定之外的其他目的，禁止接收方将共享数据再次共享给第三方；为接收方用户分配精细化的访问权限，采用多因素认证机制，确保接收方用户身份的真实性；建立共享数据访问日志审计机制，记录接收方用户的访问行为、操作内容等信息，对接收方的使用行为进行全程监督与管控。

在脱敏处理方面，根据共享数据的敏感等级与共享目的，对共享数据进行针对性的脱敏处理，确保共享数据不泄露患者隐私。对于需要对外共享的高敏感数据，必须进行彻底的脱敏处理，去除所有可识别患者身份的信息，确保脱敏后的数据无法关联到具体患者；对于内部跨部门共享的中敏感数据，可根据共享需求采用部分脱敏处理（如隐藏部分身份标识字段）；对于低敏感数据，可在确保隐私安全的前提下适当简化脱敏处理流程。同时，建立共享数据脱敏质量检验机制，由专业人员对脱敏后的共享数据进行检验，确保脱敏效果符合隐私保护要求。此外，对于涉及科研、教学等公益目的的数据共享，可采用数据信托、联邦学习等新兴技术，在不泄露原始数据的前提下实现数据的共享利用。

（六）数据销毁与归档环节隐私保护

数据销毁与归档环节的隐私保护核心是确保数据在生命周期结束后得到安全处理，防止数据残留与泄露，需分别针对销毁与归档环节制定专项防护策略。在数据销毁环节，需建立严格的医疗数据销毁管理制度，明确数据销毁的条件、流程、方式与责任主体。数据销毁条件包括数据达到法定保存期限、数据不再使用且无保存价值、存储介质报废淘汰等；数据销毁流程需经过申请、审核、批准、实施、验收等环节，确保销毁过程规范可控；数据销毁方式需根据存储介质的类型选择合适的方式，对于硬盘、U 盘等磁存储介质，采用消磁、物理粉碎等方式；对于光盘等光存储介质，采用物理粉碎、化学腐蚀等方式；对于云端存储的数据，采用彻底删除、覆盖写入等方式，确保数据无法被恢复。

数据销毁实施过程中,需安排专人监督,确保销毁操作符合要求;销毁完成后,需进行验收,出具数据销毁验收报告,记录销毁的数据名称、数量、存储介质、销毁方式、销毁时间、参与人员等信息,确保销毁过程可追溯。同时,禁止将未进行安全销毁的存储介质随意丢弃或流入市场,防止存储介质中的数据被非法获取。

在数据归档环节,需建立规范的医疗数据归档管理制度,确保归档数据的安全存储与合规管理。归档数据需经过筛选、整理、鉴定等环节,确保归档数据的完整性、准确性与可用性;采用加密存储方式对归档数据进行安全存储,选择安全可靠的归档存储介质(如磁带库、光盘库、云端归档存储),部署访问控制、安全审计等防护措施,防止归档数据被非法访问、篡改或泄露;明确归档数据的保存期限,严格按照相关法律法规与行业标准的要求保存归档数据,保存期限届满后,按照数据销毁流程进行安全销毁;建立归档数据访问审批机制,用户需要访问归档数据时,需提交访问申请,经审批通过后才能获得访问权限,同时记录访问行为,确保访问可追溯。此外,需定期对归档数据进行巡检与维护,检查归档存储介质的运行状态与数据完整性,及时发现并处置归档数据安全隐患。

三、医疗数据隐私保护技术体系建设

(一) 数据加密技术应用

数据加密技术是医疗数据隐私保护的核心技术,需根据医疗数据的全生命周期各环节特点,选择合适的加密技术,构建全方位的加密防护体系。在对称加密技术应用方面,主要用于医疗数据的传输与存储环节,采用 AES-256、SM4 等高强度对称加密算法,实现数据的快速加密与解密。例如,在医疗数据传输过程中,使用 AES-256 算法对数据进行加密,确保数据在传输过程中的安全;在本地存储环节,使用 SM4 算法对存储介质中的数据进行加密,防止存储介质被盗或丢失后数据泄露。对称加密技术的优势是加密解密效率高,适合处理大量数据,但需要加强密钥的管理,防止密钥泄露。

在非对称加密技术应用方面,主要用于身份认证、密钥交换等场景,采用 RSA-2048、ECC(椭圆曲线加密)等算法,实现数据的安全认证与密钥的安全传输。例如,在终端接入认证、跨机构数据共享身份认证等场景中,使用 RSA-2048 算法实现用户身份的数字签名与验证,确保身份的真实性;在对称加密密钥交换过

程中,使用 ECC 算法实现密钥的安全传输,防止密钥在交换过程中被拦截窃取。非对称加密技术的优势是安全性高,无需提前共享密钥,但加密解密效率较低,不适合处理大量数据,通常与对称加密技术结合使用,实现优势互补。^①

在同态加密技术应用方面,主要用于数据共享与分析场景,该技术允许在加密数据上直接进行计算,而无需解密数据,能够有效保护数据在共享分析过程中的隐私。例如,在多中心科研协作场景中,各医院的科研数据采用同态加密技术加密后,共享给科研机构,科研机构可以直接对加密数据进行统计分析,获得分析结果,而无法获取原始数据,既实现了数据的共享利用,又保护了患者隐私。目前,同态加密技术仍处于快速发展阶段,需结合医院业务需求与技术成熟度,逐步推广应用。

在区块链加密技术应用方面,利用区块链的去中心化、不可篡改、可追溯等特性,实现医疗数据的安全存储与共享。通过区块链技术为每一条医疗数据生成唯一的哈希值,记录数据的全生命周期流转信息,确保数据的完整性与可追溯性;采用区块链加密算法(如 SHA-256)对数据进行加密存储,防止数据被篡改;在数据共享场景中,通过区块链智能合约实现数据共享的自动授权与访问控制,确保数据共享安全可控。例如,在电子病历共享场景中,将电子病历数据存储在区块链上,患者可以通过智能合约授权不同的医疗机构访问自己的电子病历,实现电子病历的安全共享与隐私保护。

(二) 数据脱敏技术应用

数据脱敏技术是实现医疗数据安全共享与利用的关键技术,需根据不同的使用场景选择合适的脱敏技术,确保脱敏后的数据既符合隐私保护要求,又能满足业务使用需求。在静态脱敏技术应用方面,主要用于数据离线共享、系统测试、科研数据处理等场景,在数据脱离生产环境前对数据进行脱敏处理,生成脱敏后的数据集供使用。常用的静态脱敏技术包括替换、删除、泛化、加密、掩码等。替换技术是将敏感字段(如身份证号、姓名)替换为虚构的信息,确保无法识别到具体患者;删除技术是直接删除无关的敏感字段,减少敏感信息暴露;泛化技术是将具体的敏感数据(如具体年龄、具体地址)转化为模糊的范围信息(如年龄段、地区);掩码技术是隐藏敏感字段的部分信息(如将身份证号显示为

^① 贾未,计虹,李翠霞,等. 医疗数据共享过程中的信息安全与隐私保护 [J]. 中国数字医学, 2025, 20 (11): 19-24.

110101*****1234)。静态脱敏技术的优势是脱敏效果稳定,适合大批量数据的离线处理。

在动态脱敏技术应用方面,主要用于数据在线访问、实时查询等场景,当用户访问敏感数据时,系统根据用户的身份、权限、访问场景等信息,实时对敏感数据进行脱敏处理,用户仅能看到脱敏后的信息,而原始数据仍保持加密存储。动态脱敏技术能够确保不同用户在不同场景下看到不同粒度的敏感数据,实现“按需脱敏”。例如,普通医护人员访问患者数据时,患者的身份证号、联系方式等敏感字段被脱敏显示;管理人员进行数据统计时,仅能看到汇总数据,无法看到个体敏感数据;系统管理员进行系统维护时,所有敏感数据均被脱敏处理。动态脱敏技术的优势是不影响原始数据的存储与使用,能够实现对敏感数据的实时防护,但对系统性能有一定要求,需在系统设计阶段充分考虑。

在不可逆脱敏技术应用方面,主要用于对敏感性极高、无需逆向恢复的医疗数据(如基因数据、核心诊疗记录)的处理,通过不可逆的加密算法或哈希算法对数据进行处理,确保数据无法被逆向恢复为原始数据。例如,在科研数据共享场景中,对患者的基因数据采用 SHA-256 哈希算法进行不可逆脱敏处理,生成唯一的哈希值,科研人员仅能对哈希值进行分析,无法获取原始基因数据,有效保护患者隐私。不可逆脱敏技术的优势是安全性极高,但适用场景有限,仅适用于无需逆向恢复的数据分析场景。

在可逆脱敏技术应用方面,主要用于对需要在特定条件下逆向恢复的医疗数据的处理,通过加密、编码等可逆技术对数据进行处理,在需要使用原始数据时,可通过解密、解码等方式恢复原始数据。例如,在医疗数据归档场景中,对归档数据采用可逆加密技术进行脱敏处理,当需要查阅原始归档数据时,经审批通过后可解密恢复原始数据。可逆脱敏技术的优势是灵活性高,适合需要逆向恢复数据的场景,但需要加强密钥的管理,防止密钥泄露导致数据泄露。

(三) 访问控制技术应用

访问控制技术是规范医疗数据访问行为、防止非法访问的核心技术,需结合医院业务特点与数据分级分类结果,构建精细化的访问控制体系。在基于角色的访问控制(RBAC)技术应用方面,根据医院内部的岗位设置,将用户划分为不同的角色(如医生、护士、药师、行政人员、科研人员等),为每个角色分配固定的访问权限,用户通过所属角色获得相应的访问权限。例如,医生角色可访问

自己负责患者的诊疗记录、检查检验结果等数据；护士角色可访问患者的基本信息、护理记录等数据；行政人员角色仅能访问汇总统计数据，无法访问个体患者数据。RBAC技术的优势是易于管理，适合岗位相对固定的场景，但灵活性不足，无法满足复杂的访问控制需求。

在基于属性的访问控制（ABAC）技术应用方面，根据用户属性（如岗位、职称、所属科室）、数据属性（如数据等级、数据类型、所属业务）、环境属性（如访问时间、访问地点、访问设备）等多维度属性，动态决定用户是否具有访问权限。ABAC技术能够实现更精细化、更灵活的访问控制，适合复杂的医疗业务场景。例如，对于高敏感的患者基因数据，仅允许具备相应科研资质的科研人员在工作时间内通过医院内部授权设备访问；对于急诊患者的诊疗数据，允许急诊医生在任何时间通过授权的移动终端访问。ABAC技术的优势是灵活性高、适应性强，但配置与管理相对复杂，需建立完善的属性管理体系。

在基于区块链的访问控制技术应用方面，利用区块链的去中心化、不可篡改、智能合约等特性，实现医疗数据访问权限的分布式管理与自动控制。通过区块链记录用户的身份信息、访问权限、数据流转信息等，确保访问权限的透明性与可追溯性；利用智能合约定义访问控制规则，当用户申请访问数据时，智能合约自动验证用户的身份与权限，符合规则则自动授权访问，不符合规则则拒绝访问。例如，患者可以通过区块链智能合约授权不同的医疗机构在特定时间段内访问自己的电子病历，访问权限到期后智能合约自动回收权限，无需人工干预。基于区块链的访问控制技术能够提升访问控制的安全性及自动化水平，但目前技术成熟度有待进一步提升，需结合医院实际情况逐步应用。

在多因素认证技术应用方面，作为访问控制的重要补充，通过多种认证因素的组合，提升用户身份认证的安全性，防止账号密码被盗用。常用的认证因素包括知识因素（如账号密码）、持有因素（如动态口令令牌、手机验证码）、生物因素（如指纹识别、人脸识别、虹膜识别）等。在医疗数据访问场景中，采用“账号密码+手机验证码+指纹识别”的多因素认证方式，确保用户身份的真实性。例如，医护人员访问高敏感患者数据时，需先输入账号密码，再输入手机接收的动态验证码，最后进行指纹识别，三重认证通过后才能获得访问权限。多因素认证技术的优势是安全性高，能够有效防范账号密码泄露带来的安全风险，是医疗数据访问控制的重要保障手段。

（四）数据泄露检测与防护技术应用

数据泄露检测与防护技术是及时发现并处置医疗数据泄露事件的关键技术，需构建“事前预防、事中监测、事后处置”全流程的检测与防护体系。在数据泄露预防技术应用方面，通过数据分类分级、访问控制、加密、脱敏等技术，从源头防范数据泄露风险。同时，部署数据防泄漏（DLP）系统，对医疗数据的产生、传输、存储、使用、共享等全流程进行监控，防止敏感数据通过邮件、U 盘、网络传输等方式外泄。DLP 系统能够识别敏感数据，根据预设的规则对敏感数据的流转进行控制，例如禁止将高敏感数据拷贝到 U 盘、禁止通过非加密邮件发送敏感数据等，从源头阻断数据泄露通道。

在数据泄露监测技术应用方面，部署数据泄露检测系统，通过流量分析、行为分析、日志分析等多种技术手段，实时监测医疗数据的流转状态与用户的操作行为，及时发现数据泄露迹象。流量分析技术通过监测网络流量中是否包含敏感数据，识别数据泄露行为；行为分析技术通过建立用户正常操作行为基线，当用户操作行为偏离基线时（如非工作时间大量下载敏感数据、频繁访问与业务无关的敏感数据），及时发出告警；日志分析技术通过对用户访问日志、系统操作日志、数据传输日志等进行集中分析，发现异常操作行为与数据泄露痕迹。例如，数据泄露检测系统监测到某用户在凌晨 3 点频繁下载患者诊疗数据，且下载数据量远超正常工作需求，系统立即发出高危告警，并通知安全运维人员及时处置。

在数据泄露追溯技术应用方面，通过数据标签、区块链、日志审计等技术，实现对数据泄露事件的精准追溯。为每一条医疗数据打上唯一的数据标签，标签包含数据等级、产生时间、责任人、流转路径等信息，当发生数据泄露时，通过数据标签可快速追溯数据的来源、流转过程与相关责任人；利用区块链技术记录数据的全生命周期流转信息，区块链的不可篡改特性确保流转信息的真实性，为数据泄露追溯提供可靠依据；通过安全审计系统对用户操作日志、数据传输日志等进行详细记录，当发生数据泄露时，通过日志分析可精准定位泄露事件的时间、地点、责任人、泄露方式等信息，为事件的调查与处理提供支撑。

在数据泄露应急处置技术应用方面，部署应急响应平台，实现对数据泄露事件的快速响应与处置。应急响应平台能够自动接收数据泄露检测系统的告警信息，快速评估事件的严重程度，启动相应级别的应急响应预案；通过远程控制、权限冻结、数据隔离等技术手段，快速阻断数据泄露通道，防止泄露范围扩大；利用

数据备份恢复技术，及时恢复被泄露或篡改的数据，确保业务连续性；通过应急响应平台实现与内部各部门、外部监管机构的协同联动，提升应急处置效率。例如，当发生大规模数据泄露事件时，应急响应平台立即冻结相关用户的访问权限，隔离泄露数据所在的服务器，启动数据备份恢复流程，并及时向医院管理层与监管部门上报事件情况。

四、医疗数据合规管理体系建设

（一）合规管理核心目标与原则

医疗数据合规管理体系建设的核心目标是确保医院医疗数据的全生命周期管理符合相关法律法规、行业标准与内部管理制度要求，防范合规风险，保障医疗数据的合法合规使用，维护患者的合法权益与医院的声誉。围绕这一核心目标，合规管理体系建设需遵循“依法依规、全面覆盖、风险导向、持续改进、协同联动”五大核心原则。依法依规原则要求严格遵循《网络安全法》《数据安全法》《个人信息保护法》《医疗卫生机构网络安全管理办法》《电子病历应用规范》等相关法律法规与行业标准，将合规要求贯穿医疗数据管理全流程。

全面覆盖原则要求合规管理覆盖医疗数据的全生命周期（产生、采集、传输、存储、使用、共享、销毁、归档），覆盖医院内部所有涉及医疗数据管理的部门、岗位与人员，覆盖所有类型的医疗数据（电子病历、检查检验结果、基因数据、影像数据等），确保无合规管理盲区。风险导向原则要求以合规风险评估为基础，针对高风险环节（如数据共享、远程访问、第三方合作）、高敏感数据制定强化的合规管理措施，优先解决重大合规风险问题，提升合规管理的针对性与有效性。持续改进原则要求建立合规管理动态优化机制，根据法律法规更新、行业标准变化、业务发展需求、合规风险评估结果等，及时调整合规管理策略与措施，确保合规管理体系的时效性与适应性。协同联动原则要求加强医院内部各部门（信息科、医务科、质控科、法务科、人事科等）之间的协同配合，明确各部门的合规管理职责，形成合规管理合力；同时，加强与监管部门、行业协会、法律机构等外部机构的沟通与联动，及时掌握合规政策动态，获取合规管理支持。

（二）合规管理制度体系构建

合规管理制度体系是医疗数据合规管理的基础，需构建覆盖“基础管理、全生命周期管理、专项管理、责任追究”的全方位管理制度体系。在基础管理制度

方面,制定《医疗数据合规管理总则》,明确合规管理的目标、原则、组织架构、职责分工等,为合规管理工作提供总体指导;制定《医疗数据分级分类管理办法》,明确数据分级分类的标准、流程、标签管理等,为精准化合规管理提供依据;制定《医疗数据合规风险评估管理办法》,明确风险评估的流程、方法、频率等,及时识别与管控合规风险;制定《医疗数据合规培训管理办法》,明确培训的内容、对象、频率、考核方式等,提升全员合规意识与能力。

在全生命周期合规管理制度方面,针对医疗数据全生命周期各环节制定专项合规管理办法,确保各环节合规管理有章可循。制定《医疗数据采集合规管理办法》,规范数据采集的范围、方式、告知同意流程等;制定《医疗数据传输合规管理办法》,明确数据传输的加密要求、链路安全要求、传输校验要求等;制定《医疗数据存储合规管理办法》,规范数据存储的加密要求、访问控制要求、备份恢复要求、存储介质管理要求等;制定《医疗数据使用合规管理办法》,明确数据使用的权限管控、行为规范、脱敏要求等;制定《医疗数据共享合规管理办法》,规范数据共享的审批流程、安全协议签订、脱敏处理要求等;制定《医疗数据销毁与归档合规管理办法》,明确数据销毁的流程、方式、验收要求,以及归档数据的存储、访问、保存期限要求等。

在专项合规管理制度方面,针对特殊场景、特殊类型数据制定专项合规管理办法,提升合规管理的精准性。制定《第三方医疗数据合作合规管理办法》,规范与云服务商、软件供应商、科研协作机构、保险机构等第三方机构的数据合作行为,明确双方的合规责任与义务;制定《远程医疗数据合规管理办法》,规范远程医疗业务中数据的采集、传输、使用、共享等环节的合规要求;制定《医疗大数据分析合规管理办法》,明确医疗大数据分析过程中的数据脱敏、隐私保护、合规审批等要求;制定《患者数据权利保护管理办法》,明确患者对其数据的知情权、访问权、更正权、删除权等权利的行使流程与保障措施。

在责任追究制度方面,制定《医疗数据合规责任追究办法》,明确各部门、各岗位的合规责任,建立严格的责任追究机制。对于违反合规管理制度、导致合规风险事件发生的部门或个人,根据事件的严重程度,采取通报批评、经济处罚、岗位调整、纪律处分等措施;对于造成重大数据泄露、侵犯患者隐私等严重合规事件的,依法追究相关人员的法律责任;建立合规责任追究台账,记录责任追究的过程、结果等信息,确保责任追究可追溯。同时,建立合规管理激励机制,对

严格遵守合规管理制度、在合规管理工作中表现突出的部门或个人给予表彰与奖励，营造良好的合规管理氛围。

（三）合规管理组织架构与职责分工

构建完善的医疗数据合规管理组织架构，明确各层级、各部门的合规管理职责，确保合规管理工作有序开展。医院层面成立数据安全与合规管理委员会，作为合规管理的最高决策机构，由医院院长担任主任，分管副院长担任副主任，成员包括信息科、医务科、质控科、法务科、人事科、财务科等相关部门负责人。数据安全与合规管理委员会的主要职责包括：统筹规划合规管理体系建设，审议合规管理重大政策与制度，审批重大数据共享、第三方合作等合规事项，协调解决合规管理工作中的重大问题，监督合规管理措施的落实情况。

数据安全与合规管理委员会下设办公室，办公室设在信息科，作为合规管理的日常办事机构，配备专职的合规管理人员，负责合规管理的日常工作。办公室的主要职责包括：组织制定与修订合规管理制度，开展合规风险评估与合规检查，组织开展合规培训与宣贯，受理与处理患者数据权利相关的申请与投诉，协调各部门开展合规管理工作，向数据安全与合规管理委员会汇报合规管理工作情况。

各业务部门（如医务科、护理部、检验科、放射科、行政科室等）设立合规管理联络员，由部门负责人或业务骨干担任，负责本部门的日常合规管理工作。业务部门合规管理联络员的主要职责包括：组织本部门人员学习与遵守合规管理制度，落实本部门相关的合规管理措施，及时向数据安全与合规管理委员会办公室上报本部门的合规风险隐患与合规事件，配合开展合规检查与风险评估工作。

明确各部门的核心合规管理职责：信息科负责合规管理技术支撑，部署与维护合规管理相关的技术设备与系统，开展数据安全防护与数据泄露检测，确保数据全生命周期的技术合规；医务科负责诊疗业务相关的合规管理，规范医护人员的医疗数据采集、使用等行为，监督电子病历等诊疗数据的合规管理；质控科负责合规管理的质量监督，开展合规管理工作的质量评估与考核，确保合规管理措施的有效落实；法务科负责提供合规法律支持，解读相关法律法规与行业标准，参与合规管理制度的制定与修订，处理合规相关的法律纠纷与诉讼；人事科负责将合规管理要求纳入人员招聘、培训、考核、奖惩等环节，提升全员合规意识与能力；各临床科室、行政科室负责本部门人员的合规管理，落实本部门相关的合规管理措施，防范本部门的合规风险。

（四）合规风险评估与管控机制

建立常态化的医疗数据合规风险评估与管控机制，及时识别、评估与处置合规风险，确保合规管理体系的有效运行。在合规风险评估方面，明确风险评估的流程、方法与频率，确保风险评估工作规范开展。风险评估流程包括风险识别、风险分析、风险评价三个环节：风险识别阶段，通过问卷调查、现场检查、日志分析、专家论证等多种方式，全面识别医疗数据全生命周期各环节、各部门、各岗位存在的合规风险点（如数据采集未获得患者同意、数据共享未经过审批、数据传输未加密、第三方合作机构违规使用数据等）；风险分析阶段，对识别出的风险点进行深入分析，明确风险发生的可能性、影响程度、风险来源、风险传导路径等；风险评价阶段，根据风险分析结果，采用风险矩阵等方法对风险进行分级（如极高风险、高风险、中风险、低风险），确定风险的优先级。

风险评估频率根据风险等级与业务变化情况确定：对于极高风险、高风险环节，每季度开展一次专项风险评估；对于中风险、低风险环节，每年开展一次全面风险评估；当发生重大合规事件、法律法规更新、业务流程调整、第三方合作机构变更等情况时，及时开展专项风险评估。风险评估完成后，生成合规风险评估报告，明确风险点、风险等级、风险分析结果、管控建议等，上报数据安全与合规管理委员会审议。

在合规风险管控方面，根据风险评估结果，制定差异化的风险管控措施，确保风险得到有效处置。对于极高风险、高风险环节，采取强化的管控措施，如完善管理制度、升级技术防护手段、加强人员培训与考核、增加合规检查频率等；对于中风险、低风险环节，采取常规的管控措施，如定期开展合规检查、加强日常监督等。建立合规风险管控台账，记录风险点、管控措施、责任部门、责任人、管控期限、管控效果等信息，对风险管控过程进行全程跟踪与管理。

建立合规风险动态监测机制，实时监测风险管控措施的落实情况与风险变化趋势，及时调整管控措施。通过合规检查、日志审计、技术监测等方式，监测风险管控措施是否有效落实，是否存在新的风险点；当风险等级发生变化时，及时调整管控策略与措施；当风险得到有效控制后，及时降低风险等级或解除管控措施。同时，建立合规风险预警机制，根据风险监测结果，对可能发生的合规风险及时发出预警，通知相关部门与人员采取预防措施，防止风险事件发生。

（五）合规审计与监督机制

建立完善的医疗数据合规审计与监督机制，确保合规管理制度的有效落实与合规风险的有效管控。在合规审计方面，构建“内部审计+外部审计”相结合的审计体系，全面开展合规审计工作。内部审计由医院内部审计部门或数据安全与合规管理委员会办公室组织开展，定期对医疗数据全生命周期的合规管理情况进行审计，审计内容包括合规管理制度的落实情况、数据全生命周期各环节的合规情况、各部门与岗位的合规职责履行情况、合规风险管控措施的落实情况等。内部审计频率根据合规风险等级确定，极高风险、高风险环节每半年审计一次，中风险、低风险环节每年审计一次。

外部审计由医院聘请专业的第三方审计机构开展，每1-2年开展一次全面的医疗数据合规审计，重点审计医院医疗数据管理的合规性、合规管理体系的有效性等，为医院合规管理工作提供专业的改进建议。审计完成后，生成合规审计报告，明确审计发现的问题、整改建议、责任部门等，上报数据安全与合规管理委员会审议。针对审计发现的问题，建立整改台账，明确整改措施、责任人员、整改期限，跟踪整改落实情况，确保问题整改到位；整改完成后，开展整改效果验证，确保问题得到彻底解决。

在合规监督方面，建立“日常监督+专项监督”相结合的监督机制，加强对合规管理工作全程监督。日常监督由各部门合规管理联络员负责，对本部门的日常合规管理工作进行监督，及时发现并纠正违规行为；数据安全与合规管理委员会办公室定期对各部门的合规管理工作进行抽查，督促各部门落实合规管理要求。专项监督由数据安全与合规管理委员会办公室组织开展，针对重大合规事件、高风险环节、群众投诉举报等情况，开展专项监督检查，深入调查问题原因，明确责任主体，采取针对性的处置措施。

建立合规监督举报机制，设立专门的举报电话、邮箱等举报渠道，鼓励医院内部人员与外部人员举报医疗数据违规管理行为。对举报信息进行严格保密，及时对举报内容进行调查核实，对查实的违规行为，按照合规责任追究办法进行处理；对举报有功人员给予表彰与奖励。同时，建立合规监督通报机制，定期通报合规监督检查结果、违规行为处置情况、问题整改情况等，营造公开透明的合规监督氛围，督促各部门与人员严格遵守合规管理制度。

五、特殊场景医疗数据隐私保护与合规管理

（一）远程医疗场景

远程医疗场景涉及跨机构、跨区域的医疗数据传输与共享，数据隐私保护与合规管理面临诸多挑战，需构建“专用网络+加密传输+权限管控+合规审批”全流程的防护体系。在网络与传输安全方面，为远程医疗业务构建独立的专用网络，采用5G网络切片、VPN专线等技术，实现远程医疗数据的安全传输；对远程医疗数据采用端到端加密方式，使用高强度加密算法，确保数据在传输过程中不被拦截、窃取或篡改；部署网络安全监测设备，实时监测远程医疗网络的运行状态与数据传输情况，及时发现并处置网络攻击与数据泄露事件。

在权限管控方面，建立远程医疗数据访问权限精细化管理机制，根据远程医疗参与人员的身份（如远程医生、本地医生、护士、技术人员）、职责等，分配最小必要的访问权限；采用多因素认证机制，确保远程访问人员身份的真实性；建立远程访问权限动态调整机制，远程医疗业务结束后，及时回收访问权限，防止权限滥用。在数据共享合规方面，建立远程医疗数据共享专项审批机制，远程医疗合作双方需签订数据共享安全协议，明确双方的隐私保护责任与义务；共享数据前，对敏感数据进行脱敏处理，去除可识别患者身份的信息；建立远程医疗数据共享日志审计机制，记录数据共享的时间、内容、访问人员等信息，确保共享行为可追溯。

在合规管理方面，远程医疗数据管理需严格遵循《远程医疗服务管理规范》《互联网诊疗管理办法》等相关法律法规与行业标准，确保远程医疗业务的合法合规开展；远程医疗合作双方需明确数据主权与使用范围，禁止将远程医疗数据用于协议约定之外的其他目的；建立远程医疗数据安全事件应急响应机制，当发生数据泄露、篡改等安全事件时，合作双方需协同开展应急处置，及时上报相关监管部门。此外，需加强对远程医疗设备的安全管理，对远程手术机器人、高清会诊终端等设备进行安全加固，定期开展漏洞扫描与安全检测，防止设备被攻击导致数据泄露。

（二）医疗大数据与人工智能应用场景

医疗大数据与人工智能应用场景涉及海量医疗数据的汇聚、分析与利用，数据隐私保护与合规管理的核心是确保数据在分析利用过程中不泄露患者隐私，需

构建“数据脱敏+联邦学习+合规审批+全程审计”的防护体系。在数据预处理方面，对汇聚的医疗大数据进行彻底的脱敏处理，采用静态脱敏、动态脱敏等技术，去除患者的身份标识信息，生成可供分析利用的脱敏数据集；建立脱敏数据质量评估机制，确保脱敏后的数据既符合隐私保护要求，又能满足人工智能模型训练与数据分析的需求。

第四节 医院信息化安全应急响应与灾备恢复机制

一、医院信息化安全应急响应机制

（一）应急响应机制构建核心目标与原则

1. 核心目标

医院信息化安全应急响应机制构建的核心目标是建立“事前预防、事中处置、事后恢复”的全流程闭环管理体系，快速、有效应对各类信息化安全事件（如网络攻击、数据泄露、系统崩溃、通信中断等），最大限度降低安全事件对医疗业务开展、患者生命健康、医院声誉及数据资产的影响，保障医疗服务连续性、数据安全性和通信稳定性。具体而言，核心目标可细化为四个维度：一是快速止损，在安全事件发生初期迅速阻断风险扩散通道，避免事件影响范围扩大；二是精准处置，通过科学的应急响应流程和技术手段，精准定位事件根源，采取针对性处置措施；三是快速恢复，在事件得到控制后，尽快恢复信息系统、通信网络及医疗业务的正常运行；四是持续改进，通过对事件的复盘总结，优化应急响应机制和安全防护体系，提升医院应对信息化安全风险的综合能力。

从医疗行业特殊性出发，应急响应机制还需兼顾医疗服务的公益性和紧迫性。例如，在突发网络攻击导致急诊信息系统中断时，应急响应的首要目标是保障急诊挂号、诊疗记录、检查检验结果查询等核心业务的快速恢复，确保急诊患者得到及时救治；在发生数据泄露事件时，需优先保障患者隐私权益，及时采取数据脱敏、泄露源阻断等措施，同时按要求向监管部门和患者履行告知义务。

2. 核心原则

为实现上述核心目标，医院信息化安全应急响应机制构建需遵循“生命至上、预防为主、快速响应、协同联动、依法合规、持续优化”六大核心原则。生命至

上原则是医疗行业应急响应的首要原则，要求在应对任何信息化安全事件时，始终将保障患者生命健康放在首位，优先保障急诊、重症监护、手术麻醉等关键医疗业务的连续性，必要时可采取“业务优先于数据、救治优先于系统”的临时处置策略。

预防为主原则强调应急响应的前置性，通过常态化风险评估、安全监测、漏洞修复、应急演练等措施，从源头降低安全事件发生的可能性，提升医院对安全风险的预判和防范能力。快速响应原则要求建立扁平化的应急响应组织架构和高效的应急响应流程，明确各环节的响应时限和责任主体，确保在安全事件发生后能够第一时间启动响应、开展处置。协同联动原则要求加强医院内部各部门（信息科、医务科、护理部、后勤保障科、法务科、宣传科等）之间的协同配合，同时建立与公安、网信、卫健、通信运营商、安全服务商等外部机构的联动机制，形成应急处置合力。

依法合规原则要求应急响应全过程严格遵循《网络安全法》《数据安全法》《个人信息保护法》《医疗卫生机构网络安全管理办法》《网络安全事件应急预案》等相关法律法规和行业标准，规范应急处置流程、数据安全事件报告和信息发布等行为，确保应急响应工作合法合规。持续优化原则要求建立应急响应复盘总结机制，对每起安全事件的处置过程进行全面复盘，分析事件原因、处置成效和存在的问题，针对性地优化应急响应预案、技术手段和管理措施，提升应急响应机制的适应性和有效性。

（二）应急响应组织架构与职责分工

1. 组织架构设计

结合医院管理模式和信息化建设实际，构建“一级指挥、二级响应、三级执行”的扁平化应急响应组织架构，确保应急指令传达高效、处置责任落实到位。一级指挥机构为医院信息化安全应急响应领导小组，作为应急响应的最高决策机构，由医院院长担任组长，分管副院长担任副组长，成员包括信息科、医务科、护理部、后勤保障科、法务科、宣传科、财务科、保卫科及各临床科室负责人。

二级响应机构为应急响应办公室和专项应急工作组，应急响应办公室设在信息科，作为日常办事机构，配备专职应急管理人员，负责应急响应的统筹协调、预案管理、演练组织、信息汇总等工作；专项应急工作组根据安全事件类型划分为网络攻击应急组、数据安全应急组、系统故障应急组、通信中断应急组、医疗

业务保障组、后勤支撑组、法务合规组、宣传舆情组，各专项组由相关部门负责人担任组长，成员由具备相应专业能力的人员组成。

三级执行机构为各科室应急联络员队伍，由各临床科室、行政科室指定专人担任，负责本科室安全事件的初步排查、信息上报、应急处置配合及本科室人员的应急动员等工作。通过三级组织架构的构建，形成“领导小组统筹决策、办公室协调推进、专项组精准处置、联络员基层联动”的应急响应工作格局。

2. 各层级职责分工

应急响应领导小组的核心职责包括：审定医院信息化安全应急响应预案及相关管理制度；统一指挥和协调各类信息化安全事件的应急处置工作；决定启动和终止应急响应级别；审批应急处置过程中的重大决策（如系统停机、数据恢复、外部支援请求等）；负责向卫健、网信、公安等上级监管部门汇报事件情况及处置进展；协调解决应急处置过程中的资源保障和跨部门重大问题；审定应急处置工作总结和预案优化方案。

应急响应办公室的核心职责包括：负责应急响应预案的制定、修订、备案和管理工作；组织开展常态化应急演练、安全培训和应急物资储备管理；负责安全事件的信息汇总、分析和上报，及时向领导小组和各专项工作组传递应急指令和处置信息；协调各专项工作组开展应急处置工作，跟踪处置进展，督促责任落实；负责应急处置过程的文档记录和档案管理；组织应急处置复盘总结，提出预案优化和安全防护改进建议。

各专项应急工作组的职责分工明确且各有侧重：网络攻击应急组（由信息科网络安全人员牵头）负责网络攻击事件的监测、预警、溯源和处置，包括 DDoS 攻击、恶意入侵、病毒感染等，采取防火墙策略调整、入侵阻断、病毒查杀等技术措施，恢复网络正常运行；数据安全应急组（由信息科数据管理人员和法务科人员牵头）负责数据泄露、篡改、丢失等数据安全事件的处置，包括泄露源定位、数据脱敏、数据恢复、责任追溯等，同时负责配合监管部门调查和患者权益保障工作；系统故障应急组（由信息科系统运维人员牵头）负责 HIS、LIS、PACS、电子病历等核心业务系统故障的应急处置，包括系统故障排查、漏洞修复、系统重启和数据恢复等，保障业务系统快速恢复正常；

通信中断应急组（由信息科通信管理人员和通信运营商对接人员牵头）负责院内局域网、广域网、无线网络、语音通信等通信网络中断的应急处置，包括通

信链路排查、故障修复、备用通信链路切换等，保障通信网络畅通；医疗业务保障组（由医务科和护理部人员牵头）负责应急处置过程中医疗业务的统筹协调，制定业务连续性保障方案，指导临床科室开展手工诊疗记录、应急挂号等临时业务，确保医疗服务不中断；后勤支撑组（由后勤保障科人员牵头）负责应急处置过程中的电力保障、设备维修、场地安全等后勤支撑工作，确保应急处置所需的电力、设备、场地等资源及时到位；法务合规组（由法务科人员牵头）负责应急处置过程的法律合规审核，指导开展事件报告、信息发布等合规工作，处理可能引发的法律纠纷；宣传舆情组（由宣传科人员牵头）负责应急事件的舆情监测和引导，及时发布权威信息，回应社会关切，避免负面舆情扩散。

各科室应急联络员的核心职责包括：负责本科室信息化设备和系统的日常安全巡查，及时发现并上报安全隐患；在安全事件发生后，第一时间向应急响应办公室上报事件情况（包括事件发生时间、地点、影响范围、初步判断等）；配合各专项应急工作组开展事件排查和处置工作，提供本科室相关业务信息和数据；组织本科室人员学习应急响应预案和处置流程，参与应急演练；在业务系统中断时，指导本科室人员开展手工诊疗记录等临时工作，保障医疗业务连续性。

（三）应急响应分级标准与启动流程

1. 应急响应分级标准

结合医院信息化系统的重要程度、安全事件的影响范围、危害程度和处置难度，参考国家网络安全事件分级标准，将医院信息化安全应急响应划分为四级：

I级（特别重大）、II级（重大）、III级（较大）、IV级（一般）。

I级（特别重大）安全事件：指造成医院核心业务系统（如急诊系统、重症监护系统、手术麻醉系统、HIS核心模块）全面中断，且持续时间超过4小时，严重影响全院医疗服务开展，可能导致患者生命健康受到重大威胁；或发生大规模患者数据泄露（泄露数量超过10000条），可能引发重大舆情和法律风险；或遭受国家级、有组织的高强度网络攻击，导致医院信息化体系濒临崩溃。例如，勒索病毒攻击导致全院HIS、电子病历系统瘫痪，无法开展挂号、诊疗、收费等核心业务；患者基因数据、核心诊疗记录等高度敏感数据大规模泄露，被恶意传播。

II级（重大）安全事件：指造成医院多个重要业务系统（如PACS、LIS、住院管理系统）中断，持续时间2-4小时，影响多个临床科室医疗服务开展，可

能导致患者诊疗延迟；或发生较大规模患者数据泄露（泄露数量 5000-10000 条），可能引发较大舆情风险；或遭受有组织的网络攻击，导致部分核心数据被篡改或窃取。例如，网络入侵导致 PACS 系统瘫痪，影像检查无法开展，影响门诊和住院患者诊疗；部分住院患者的身份信息和诊疗记录泄露，引发患者投诉和媒体关注。

Ⅲ级（较大）安全事件：指造成单个重要业务系统或多个普通业务系统中断，持续时间 1-2 小时，影响单个科室或少数几个科室的医疗服务开展；或发生小规模患者数据泄露（泄露数量 1000-5000 条），可能引发局部舆情风险；或遭受一般性网络攻击，未造成核心数据泄露但影响系统正常运行。例如，LIS 系统故障导致检验结果无法正常传输，影响检验科和相关临床科室工作；个别科室的患者联系方式等一般敏感数据泄露，引发少量患者投诉。

Ⅳ级（一般）安全事件：指造成单个普通业务系统中断，持续时间不足 1 小时，仅影响个别岗位的工作；或发生极小规模数据泄露（泄露数量少于 1000 条），未引发舆情风险；或发现安全漏洞但未被利用，未造成实际损失。例如，医院官网后台系统故障，持续 30 分钟后恢复，未影响核心医疗业务；个别患者的挂号信息泄露，未被恶意使用。

2. 应急响应启动流程

建立“监测预警—事件报告—级别判定—启动响应”的标准化应急响应启动流程，确保应急响应启动及时、规范、高效。第一步，监测预警。通过网络安全监测平台、系统运维监控工具、日志审计系统等技术手段，对医院信息化系统、网络链路、数据资产进行 24 小时实时监测，及时发现安全异常情况（如网络流量突变、系统漏洞告警、数据访问异常、服务响应超时等）；同时，各科室应急联络员负责本科室日常安全巡查，发现安全问题及时上报。应急响应办公室对监测到的异常信息进行初步核实和分析，对可能引发安全事件的风险及时发出预警通知。

第二步，事件报告。安全事件发生后，发现人（包括系统运维人员、科室应急联络员、医护人员等）需在 15 分钟内通过应急响应热线、专用邮箱、应急管理平台等指定渠道向应急响应办公室上报事件信息。上报信息需包括：事件发生时间、地点、涉及系统/业务、影响范围、初步描述（如系统中断、数据泄露、网络攻击等）、已采取的临时措施等。对于Ⅰ级、Ⅱ级重大安全事件，应急响应

办公室需在 30 分钟内上报应急响应领导小组，并同步向上级卫健、网信部门初步报备。

第三步，级别判定。应急响应办公室接到事件报告后，立即组织相关专项应急工作组对事件进行评估，结合应急响应分级标准，初步判定事件等级，并将评估结果和等级建议上报应急响应领导小组。应急响应领导小组在接到报告后，对于Ⅰ级、Ⅱ级事件需在 30 分钟内完成等级审定，对于Ⅲ级、Ⅳ级事件需在 1 小时内完成等级审定。等级审定需综合考虑事件影响范围、危害程度、处置难度、持续时间等因素，确保等级判定准确。

第四步，启动响应。应急响应领导小组根据等级审定结果，下达应急响应启动指令。Ⅰ级、Ⅱ级应急响应由领导小组组长（院长）签发启动指令，Ⅲ级、Ⅳ级应急响应由领导小组副组长（分管副院长）签发启动指令。应急响应办公室接到启动指令后，立即通过应急指挥平台、工作群、电话等方式通知各专项应急工作组和相关科室启动应急处置工作，并发布应急响应启动公告，明确响应级别、处置要求和注意事项。应急响应启动后，各专项工作组需立即到位开展处置工作，并每 30 分钟（Ⅰ级、Ⅱ级）或 1 小时（Ⅲ级、Ⅳ级）向应急响应办公室上报处置进展。

（四）应急响应全流程处置规范

1. 事前预防与准备阶段

事前预防与准备是应急响应的基础，核心是提升医院对安全事件的预判能力和应急处置准备水平，具体工作包括：一是常态化风险评估与漏洞管理。每月开展一次信息化安全风险专项评估，每季度开展一次全面风险评估，重点排查网络架构、系统漏洞、数据安全、访问控制等方面的风险点，建立风险台账，制定整改措施，明确整改时限和责任人；与专业安全服务商合作，定期开展渗透测试和漏洞扫描，及时发现并修复高危漏洞，从源头降低安全事件发生风险。

二是应急物资储备管理。建立应急物资储备清单，明确储备物资的种类、数量、规格、存放位置和管理责任人，储备物资包括：备用服务器、交换机、路由器、防火墙等网络设备；备用硬盘、U 盘、移动存储设备等存储介质；应急发电设备、UPS 电源等电力保障设备；应急通信设备（如卫星电话、备用光纤链路、4G/5G 路由器）；操作系统、数据库、业务系统等软件安装介质和备份许可；应急处置工具（如病毒查杀软件、漏洞修复工具、数据恢复工具）；个人防护装备

和应急办公物资等。建立应急物资定期检查和更新机制，每半年对储备物资进行一次全面检查，确保物资完好可用，对过期、损坏的物资及时更换补充。

三是应急队伍建设与培训。组建由信息科专业人员、各科室技术骨干、外部安全专家组成的应急处置队伍，明确队伍成员的职责和分工；制定年度应急培训计划，每月开展一次内部安全培训（内容包括应急响应流程、技术处置方法、安全防护知识等），每季度邀请外部安全专家开展一次专项培训（内容包括最新网络攻击手段、数据安全防护技术、应急处置案例分析等）；建立培训考核机制，确保应急处置人员熟练掌握应急响应流程和技术手段，提升应急处置能力。

四是应急演练组织与评估。制定年度应急演练计划，明确演练主题、类型、时间、参与人员和评估标准，演练类型包括桌面推演、实战演练、综合演练等；每半年开展一次专项应急演练（如网络攻击应急演练、系统故障应急演练、数据泄露应急演练等），每年开展一次综合应急演练，模拟真实安全事件场景，检验应急响应组织架构、流程和处置能力；演练结束后，组织开展演练评估，分析演练过程中存在的问题，提出改进措施，优化应急响应预案和处置流程。

2. 事中处置阶段

事中处置是应急响应的核心环节，需遵循“快速定位、精准阻断、科学处置、优先保供”的原则，根据事件类型和等级采取针对性的处置措施。一是事件核实与定位。专项应急工作组接到应急响应指令后，立即开展事件核实和定位工作，通过系统日志分析、网络流量监测、现场排查等方式，明确事件类型（如网络攻击、系统故障、数据泄露、通信中断）、发生根源（如病毒感染、漏洞利用、设备故障、人为操作失误、外部攻击）、影响范围（涉及的系统、业务、科室、患者数量）和危害程度。例如，网络攻击应急组通过防火墙日志和入侵检测系统告警，定位攻击来源 IP、攻击类型和攻击目标；数据安全应急组通过数据访问日志和数据审计系统，定位数据泄露的源头和泄露数据的类型、数量。

二是风险阻断与控制。在明确事件根源和影响范围后，立即采取风险阻断措施，防止事件影响扩大。针对网络攻击事件，采取关闭攻击入口、调整防火墙策略、阻断攻击源 IP、启用入侵防御系统等措施，阻断攻击行为；针对系统故障事件，采取停止相关系统服务、隔离故障设备、关闭异常进程等措施，防止故障扩散；针对数据泄露事件，采取关闭泄露数据的访问权限、暂停相关数据传输服务、对泄露数据进行脱敏处理等措施，阻断数据进一步泄露；针对通信中断事件，采取

切换备用通信链路、重启通信设备、修复通信线路等措施,尽快恢复通信畅通。在风险阻断过程中,需优先保障急诊、重症监护等核心医疗业务的运行,必要时可采取“断网保业务”“手工替代系统”等临时措施。

三是技术处置与修复。风险阻断后,专项应急工作组开展技术处置和修复工作,根据事件类型采取针对性的技术措施。针对网络攻击事件,在阻断攻击后,对被攻击系统和设备进行安全扫描和漏洞修复,清除恶意程序和后门,恢复系统和网络的正常运行;针对系统故障事件,对故障设备和系统进行检修,修复系统漏洞,恢复系统配置,重启系统服务,确保系统正常运行;针对数据泄露事件,在阻断泄露后,对泄露数据进行全面排查,评估数据泄露的影响,采取数据恢复、数据加密、访问权限调整等措施,加强数据安全防护;针对通信中断事件,对通信线路和设备进行检修,修复故障点,切换回主用通信链路(如备用链路已启用),确保通信网络稳定运行。在技术处置过程中,需做好详细的处置记录,包括处置措施、操作时间、操作人员、处置效果等,确保处置过程可追溯。

四是业务连续性保障。在技术处置和系统修复过程中,医疗业务保障组需统筹协调各临床科室,制定业务连续性保障方案,确保医疗服务不中断。对于核心医疗业务系统中断的情况,指导临床科室开展手工诊疗记录、应急挂号、手工收费等临时业务,配备必要的手工记录表格和应急办公物资;协调检验、检查科室采用临时方式传递检验结果和影像报告(如纸质报告、电话通知);保障急诊患者的优先救治,开通急诊绿色通道,确保急诊患者能够及时得到诊疗服务。同时,加强各科室之间的沟通协调,及时传递应急处置进展和业务保障信息,确保医疗服务有序开展。

3. 事后恢复与总结阶段

事后恢复与总结是应急响应的收尾环节,核心是尽快恢复业务正常运行,总结经验教训,提升应急响应能力。一是系统与业务恢复。在技术处置完成后,专项应急工作组对系统和网络进行全面测试,验证系统功能、数据完整性和网络稳定性,确保系统和网络能够正常运行;医疗业务保障组指导各科室逐步恢复正常业务,从手工业务切换回系统业务,核对手工记录数据与系统数据的一致性,确保数据完整准确;应急响应办公室组织开展恢复效果评估,收集各科室的反馈意见,及时解决恢复过程中存在的问题。对于Ⅰ级、Ⅱ级安全事件,系统和业务恢复后,需持续监测24小时以上,确保无异常情况;对于Ⅲ级、Ⅳ级安全事件,需持续监测12小时以上。

二是事件调查与溯源。系统和业务恢复后，应急响应办公室组织各专项应急工作组开展事件调查与溯源工作，深入分析事件发生的根本原因（如技术漏洞、管理缺陷、人为失误、外部攻击等），明确事件责任主体（如内部人员、外部攻击者、设备供应商等），评估事件造成的损失（如经济损失、声誉影响、患者权益损害等）。对于涉及外部攻击的事件，及时向公安部门报案，提供事件调查资料和溯源证据，配合公安部门开展调查取证工作；对于涉及内部管理缺陷或人为失误的事件，明确相关部门和人员的责任，提出责任追究建议。

三是总结复盘与改进。应急响应办公室组织开展事件总结复盘工作，召集各专项应急工作组、相关科室负责人和应急处置人员，全面复盘事件处置过程，分析处置过程中存在的问题（如应急响应流程不顺畅、技术处置手段不足、部门协同配合不够、应急物资储备不足等），总结处置经验和教训；根据复盘结果，制定改进措施，优化应急响应预案、组织架构、处置流程和技术手段；加强对应急处置人员的培训和演练，提升应急响应能力；完善安全防护体系，修复技术漏洞，强化管理措施，从源头降低安全事件再次发生的风险。

四是信息发布与报备。按照依法合规原则，宣传舆情组负责应急事件的信息发布工作，根据事件等级和影响范围，及时通过医院官网、官方微信公众号、新闻发布会等渠道发布事件处置进展和结果，回应社会关切，避免负面舆情扩散；法务合规组负责向卫健、网信、公安等上级监管部门提交事件处置报告，按要求完成事件报备工作。信息发布和报备需遵循“真实、准确、及时、规范”的原则，避免发布虚假信息或遗漏重要信息。

（五）不同类型安全事件应急处置预案

1. 网络攻击事件应急处置预案

网络攻击事件包括 DDoS 攻击、恶意入侵、病毒感染、勒索病毒攻击、木马植入等，需针对不同攻击类型制定专项处置措施。一是 DDoS 攻击应急处置。网络攻击应急组发现 DDoS 攻击后，立即通过流量清洗设备对攻击流量进行过滤，调整防火墙策略，阻断攻击源 IP；启用备用网络带宽和冗余链路，保障核心业务系统的网络访问；联系通信运营商和 DDoS 防护服务商，请求外部技术支援，扩大流量清洗能力；持续监测网络流量变化，直至攻击停止，网络恢复正常。在处置过程中，优先保障急诊、重症监护等核心医疗业务的网络带宽，确保核心业务不受影响。

二是恶意入侵应急处置。网络攻击应急组通过入侵检测系统和日志分析,发现恶意入侵行为后,立即关闭入侵入口(如关闭相关端口、删除恶意账号等),隔离被入侵的系统和设备,防止入侵扩散;对被入侵系统进行全面扫描,清除恶意程序、后门和木马,修复系统漏洞;恢复被篡改的系统配置和数据(从备份中恢复);对入侵行为进行溯源,收集入侵证据,向公安部门报案。在处置过程中,需做好被入侵系统的隔离工作,避免入侵扩散到其他系统。

三是病毒感染应急处置。网络攻击应急组发现病毒感染后,立即隔离被感染的设备(如计算机、服务器、移动终端),断开设备与网络的连接;对被感染设备进行病毒查杀,清除病毒程序;对全院网络和设备进行全面病毒扫描,排查其他被感染设备;修复系统漏洞,更新病毒库,加强病毒防护措施;恢复被病毒破坏的数据(从备份中恢复)。对于勒索病毒感染,严禁支付赎金,立即隔离被感染设备,联系安全服务商开展病毒解密和数据恢复工作,同时向公安部门报案。

2. 系统故障应急处置预案

系统故障包括核心业务系统(HIS、LIS、PACS、电子病历系统)故障、数据库故障、服务器故障等,需根据系统重要程度和故障类型采取针对性处置措施。一是核心业务系统故障应急处置。系统故障应急组发现核心业务系统故障后,立即停止系统服务,开展故障排查,明确故障原因(如软件故障、硬件故障、配置错误等);如果是软件故障,修复软件漏洞,重启系统服务;如果是硬件故障,更换故障硬件(如服务器、硬盘等),恢复系统配置;如果故障无法短时间修复,立即启动备用业务系统,切换核心业务至备用系统运行;恢复系统数据(从备份中恢复),验证数据完整性和系统功能;系统恢复正常后,持续监测系统运行状态,确保无异常。在处置过程中,医疗业务保障组指导各科室开展手工诊疗记录等临时业务,确保医疗服务连续性。

二是数据库故障应急处置。系统故障应急组发现数据库故障后,立即停止数据库服务,开展故障排查,明确故障原因(如数据库崩溃、数据损坏、日志丢失等);如果是数据库软件故障,修复软件漏洞,重启数据库服务;如果是数据损坏,从备份中恢复数据库数据,验证数据完整性;如果故障无法短时间修复,启动备用数据库,切换业务系统至备用数据库运行;数据库恢复正常后,对数据库进行全面优化和备份,加强数据库安全防护措施。

3. 数据安全事件应急处置预案

数据安全事件包括数据泄露、数据篡改、数据丢失等，需优先保障患者隐私权益，采取针对性的处置措施。一是数据泄露应急处置。数据安全应急组发现数据泄露后，立即关闭泄露数据的访问权限，暂停相关数据传输服务，阻断数据进一步泄露；开展数据泄露溯源，通过数据访问日志和审计记录，明确泄露源（如系统漏洞、人为操作失误、外部攻击）、泄露数据的类型（如患者身份信息、诊疗记录、基因数据）和数量；对泄露数据进行评估，判断数据泄露的影响范围和危害程度；如果泄露数据涉及患者隐私，及时采取数据脱敏、删除泄露数据副本等措施，保障患者隐私权益；按要求向监管部门和患者履行告知义务，发布数据泄露事件公告，回应患者关切；配合监管部门开展调查，追究相关责任人的责任。

二是数据篡改应急处置。数据安全应急组发现数据篡改后，立即停止相关数据服务，隔离被篡改的数据；开展数据篡改溯源，明确篡改者（内部人员、外部攻击者）、篡改时间和篡改内容；从备份中恢复被篡改的数据，验证数据完整性；加强数据访问控制和审计措施，调整数据访问权限，防止再次发生数据篡改；对篡改行为进行调查，追究相关责任人的责任，涉及外部攻击的，向公安部门报案。

三是数据丢失应急处置。数据安全应急组发现数据丢失后，立即开展数据丢失原因排查，明确数据丢失的原因（如存储设备故障、人为误删除、病毒破坏等）；从备份中恢复丢失的数据，验证数据完整性；如果备份数据无法恢复，联系专业数据恢复服务商开展数据恢复工作；加强数据备份和存储管理措施，完善数据备份策略，定期开展数据恢复测试，确保数据安全。

4. 通信中断应急处置预案

通信中断包括局域网中断、广域网中断、无线网络中断、语音通信中断等，需优先保障核心医疗业务的通信畅通。一是局域网中断应急处置。通信中断应急组发现局域网中断后，立即开展故障排查，明确故障原因（如交换机故障、路由器故障、网络线路故障等）；如果是设备故障，更换故障设备，重启网络设备；如果是线路故障，修复网络线路，重新连接网络；如果故障无法短时间修复，启用备用局域网，切换核心业务至备用局域网运行；持续监测网络运行状态，确保局域网恢复正常。在处置过程中，保障急诊、重症监护等核心科室的局域网访问权限，确保核心医疗业务正常开展。

二是广域网中断应急处置。通信中断应急组发现广域网中断后，立即联系通

信运营商，排查故障原因（如线路故障、运营商设备故障等）；启用备用广域网链路（如备用光纤、4G/5G 专线），切换核心业务至备用链路运行；持续与通信运营商沟通，跟踪故障修复进展；广域网恢复正常后，切换回主用链路运行，对备用链路进行测试和维护，确保备用链路可用。

三是语音通信中断应急处置。通信中断应急组发现语音通信中断后，立即开展故障排查，明确故障原因（如电话交换机故障、线路故障等）；如果是设备故障，修复或更换电话交换机；如果是线路故障，联系通信运营商修复线路；启用备用语音通信设备（如卫星电话、应急对讲机），保障核心科室（急诊、手术室、重症监护室）的语音通信畅通；语音通信恢复正常后，对语音通信系统进行全面测试和维护，确保系统稳定运行。

二、医院信息化灾备恢复机制

（一）灾备恢复机制构建核心目标与原则

1. 核心目标

医院信息化灾备恢复机制构建的核心目标是建立“多层级、全覆盖、高可靠”的灾备体系，确保在遭遇自然灾害（如地震、洪水、台风）、人为灾难（如恶意破坏、重大操作失误）、技术灾难（如系统崩溃、数据损坏、网络瘫痪）等灾难事件时，能够快速、准确、完整地恢复医院信息化系统和数据，保障医疗业务的连续性，最大限度降低灾难事件对医疗服务、患者生命健康和医院声誉的影响。具体而言，核心目标可细化为三个维度：一是数据安全保障，确保医院核心数据（如电子病历、诊疗记录、患者信息、财务数据）的完整性、可用性和安全性，在灾难事件中不丢失、不损坏；二是业务快速恢复，明确不同业务系统的恢复优先级和恢复时间目标，确保核心医疗业务在最短时间内恢复正常运行；三是灾备体系可靠，确保灾备系统、备份数据和恢复流程的可靠性，通过常态化测试和维护，提升灾备体系的应急响应能力。

结合医院业务的特殊性，灾备恢复机制还需重点保障急诊、重症监护、手术麻醉、检验检查等核心业务的灾备恢复优先级，确保在灾难事件发生后，这些直接关系患者生命健康的业务能够优先恢复运行。同时，需保障灾备数据的隐私安全，防止在灾备存储和恢复过程中发生数据泄露。

2. 核心原则

医院信息化灾备恢复机制构建需遵循“统筹规划、分级建设、数据优先、业务连续、因地制宜、持续优化”六大核心原则。统筹规划原则要求结合医院信息化建设规划和业务发展需求，制定统一的灾备恢复体系建设规划，明确灾备建设的目标、范围、层级和实施步骤，避免重复建设和资源浪费。分级建设原则要求根据业务系统的重要程度、数据的敏感程度和恢复优先级，构建分级分类的灾备体系，对核心业务系统和高敏感数据采用高级别灾备方案，对普通业务系统和一般数据采用适度级别灾备方案，提升灾备资源的利用效率。

数据优先原则要求将数据灾备作为灾备恢复机制的核心，优先保障核心数据的备份和恢复，确保数据的完整性和可用性，为业务恢复提供数据支撑。业务连续原则要求灾备恢复机制不仅关注数据备份，更注重业务的快速恢复，通过构建高可用的灾备系统，缩短业务中断时间，保障医疗业务连续性。因地制宜原则要求结合医院的地理位置、场地条件、资金预算、技术能力等实际情况，选择合适的灾备模式和技术方案，避免盲目追求高级别灾备而忽视实际需求和可行性。持续优化原则要求建立灾备体系常态化测试、维护和优化机制，定期检查灾备系统运行状态、备份数据完整性和恢复流程有效性，根据业务发展和技术变化，及时调整灾备方案，提升灾备恢复机制的适应性和可靠性。

（二）灾备体系分级与建设标准

1. 灾备体系分级标准

参考国际灾备标准（SHARE 78）和国内行业规范，结合医院业务实际，将医院信息化灾备体系划分为五个级别：0级（无灾备）、1级（本地数据备份）、2级（本地热备）、3级（异地冷备）、4级（异地热备），明确各级别灾备体系的建设要求和适用范围。

0级（无灾备）：无任何灾备措施，仅依靠系统自身的容错能力，数据和业务无任何保护。该级别适用于无重要数据的辅助业务系统（如医院内部通知发布系统），但在医院核心业务系统中严禁采用。

1级（本地数据备份）：对核心数据进行本地备份（如定时备份到本地硬盘、磁带库），但无备用系统和异地备份。该级别能够保障数据在本地故障时的恢复，但无法应对自然灾害、机房火灾等区域性灾难。适用于普通业务系统（如医院图书馆管理系统），核心业务系统需至少采用更高级别灾备。

2级(本地热备):在本地机房构建备用系统(如双机热备、集群系统),核心数据实时同步到备用系统,具备本地快速切换能力。该级别能够应对单个设备或系统故障,实现本地业务快速恢复,但无法应对区域性灾难。适用于重要业务系统(如LIS、PACS系统)。

3级(异地冷备):在异地建立灾备机房,核心数据定时备份到异地灾备中心,具备异地数据恢复能力,但无备用业务系统或备用系统处于冷启动状态。该级别能够应对区域性灾难,保障数据不丢失,但业务恢复时间较长(数小时到数天)。适用于核心业务系统的基础灾备需求(如HIS系统的异地冷备)。

4级(异地热备):在异地建立灾备机房,构建与主机房一致的备用业务系统,核心数据实时同步到异地灾备中心,具备异地快速切换能力。该级别能够应对各类灾难事件,实现核心业务的快速恢复(分钟级到小时级),是医院核心业务系统的理想灾备级别(如急诊系统、电子病历系统的异地热备)。

2. 不同级别灾备体系建设要求

1级(本地数据备份)建设要求:制定明确的数据备份策略,核心数据采用“每日全量备份+每小时增量备份”的备份方式;备份数据存储在本地可靠的存储介质(如磁带库、磁盘阵列)中,备份介质进行加密存储和专人保管;定期开展备份数据恢复测试,确保备份数据的完整性和可用性;建立备份数据管理台账,记录备份时间、备份内容、备份介质、恢复测试结果等信息。

2级(本地热备)建设要求:在本地机房部署双机热备或集群系统,主备服务器实时同步数据和系统状态;采用共享存储或分布式存储技术,确保数据实时可用;配置自动切换软件,当主服务器发生故障时,能够自动切换到备用服务器,业务中断时间控制在分钟级以内;建立本地热备系统运维管理制度,定期检查主备服务器运行状态和数据同步情况,确保热备系统可靠运行。

3级(异地冷备)建设要求:选择距离主机房至少50公里以上的异地场地建设灾备机房,灾备机房具备独立的电力、空调、消防等基础设施;部署异地备份存储设备,核心数据通过专线或加密网络定时同步到异地灾备中心;制定异地数据恢复流程,明确数据恢复的步骤、责任人和时间要求;定期开展异地数据恢复测试,检验异地备份数据的完整性和恢复效率;建立灾备机房运维管理制度,确保灾备存储设备正常运行。

4级(异地热备)建设要求:异地灾备机房的基础设施配置与主机房一致,具

备相同的网络架构、服务器配置和存储设备；采用实时数据同步技术（如同步复制、异步复制），将核心数据实时同步到异地灾备中心，数据同步延迟控制在秒级以内；部署与主系统一致的备用业务系统，备用系统处于实时运行状态，具备与主系统相同的业务处理能力；配置自动切换系统，当主机房发生灾难时，能够自动切换到异地灾备中心，业务中断时间控制在小时级以内；建立主备机房协同运维机制，定期开展主备切换测试，确保异地热备系统的可靠性和业务恢复能力。

（三）灾备恢复关键技术体系建设

1. 数据备份技术应用

数据备份技术是灾备恢复机制的核心技术，需根据数据类型和备份需求选择合适的备份技术，构建“全量备份+增量备份+差异备份”的多层级备份体系。一是全量备份技术，指对整个数据集合进行完整备份，备份数据完整、独立，恢复时无需依赖其他备份数据。全量备份技术适用于核心数据的定期完整备份（如每日凌晨开展的全量备份），常用的技术包括磁盘阵列备份、磁带库备份、云备份等。例如，采用磁盘阵列备份技术，将 HIS 系统的全部数据备份到本地磁盘阵列中，确保数据的完整存储。

二是增量备份技术，指仅对上次备份后新增或修改的数据进行备份，备份数据量小、备份时间短，占用存储资源少。增量备份技术适用于核心数据的实时或准实时备份（如每小时开展的增量备份），常用的技术包括数据库增量备份、文件系统增量备份等。例如，采用数据库增量备份技术，对电子病历系统的数据库进行每小时增量备份，确保新增诊疗数据及时备份。

三是差异备份技术，指对上次全量备份后新增或修改的数据进行备份，备份数据量介于全量备份和增量备份之间，恢复时仅需依赖上次全量备份和最新差异备份。差异备份技术适用于核心数据的定期备份（如每日中午开展的差异备份），可作为全量备份和增量备份的补充，提升数据恢复效率。例如，采用文件系统差异备份技术，对 PACS 系统的影像文件进行每日中午的差异备份，确保影像数据的及时备份。

同时，需采用数据加密技术对备份数据进行加密存储（如采用 AES-256 加密算法），防止备份数据泄露；采用数据校验技术（如 MD5、SHA-256 校验），确保备份数据的完整性；采用备份介质管理技术，对备份磁带、硬盘等介质进行全生命周期管理，确保备份介质的安全可靠。

2. 数据同步技术应用

数据同步技术是实现本地热备和异地热备的关键技术，需根据灾备级别和业务需求选择合适的同步技术，确保数据实时或准实时同步。一是同步复制技术，指主系统数据写入的同时，实时同步到备用系统，数据同步延迟为零，确保主备系统数据完全一致。同步复制技术适用于本地热备和近距离异地热备（如主备机房距离在 10 公里以内），常用的技术包括存储区域网络（SAN）同步复制、数据库同步复制等。例如，在本地机房的双机热备系统中，采用 SAN 同步复制技术，将主服务器的数据实时同步到备用服务器，确保主备系统数据一致。

二是异步复制技术，指主系统数据写入后，通过异步方式将数据同步到备用系统，数据同步延迟在秒级以内，能够平衡数据一致性和系统性能。异步复制技术适用于远距离异地热备（如主备机房距离在 50 公里以上），常用的技术包括广域网异步复制、云同步复制等。例如，在异地热备系统中，采用广域网异步复制技术，将主机房的核心数据同步到异地灾备中心，数据同步延迟控制在 5 秒以内，既确保数据的及时性，又避免对主系统性能造成影响。

三是近同步复制技术，指主系统数据写入后，在极短时间内（毫秒级）同步到备用系统，数据同步延迟介于同步复制和异步复制之间，兼顾数据一致性和系统性能。近同步复制技术适用于对数据一致性要求较高的异地热备场景，常用的技术包括数据库近同步复制、存储近同步复制等。例如，在电子病历系统的异地热备中，采用数据库近同步复制技术，确保患者诊疗数据能够快速同步到异地灾备中心，保障数据一致性。

3. 业务切换与恢复技术应用

业务切换与恢复技术是实现灾备系统快速切换和业务恢复的关键技术，需根据灾备级别和业务需求选择合适的切换技术，缩短业务中断时间。一是自动切换技术，指通过切换软件或硬件设备，在主系统发生故障时，自动检测故障并切换到备用系统，无需人工干预，业务中断时间控制在分钟级以内。自动切换技术适用于本地热备和异地热备系统，常用的技术包括双机热备自动切换、集群系统自动切换、异地灾备自动切换等。例如，在本地热备系统中，采用双机热备自动切换软件，当主服务器发生故障时，自动切换到备用服务器，业务中断时间不超过 5 分钟。

二是手动切换技术，指通过人工操作，在主系统发生故障时，将业务切换到

备用系统，业务中断时间相对较长（数分钟到数小时）。手动切换技术适用于异地冷备和对切换精度要求较高的场景，常用的技术包括手动启动备用系统、手动配置网络参数、手动恢复数据等。例如，在异地冷备系统中，当主机房发生灾难时，通过人工操作启动异地灾备中心的备用系统，恢复备份数据，配置网络参数，将业务切换到备用系统运行。

三是快速恢复技术，指通过数据压缩、并行恢复、增量恢复等技术，提升数据恢复效率，缩短业务恢复时间。快速恢复技术适用于各类灾备系统，常用的技术包括数据库快速恢复、文件系统并行恢复、增量数据快速恢复等。例如，采用数据库并行恢复技术，同时恢复多个数据文件，提升数据恢复效率；采用增量数据快速恢复技术，仅恢复上次备份后新增或修改的数据，缩短恢复时间。

4. 灾备监控与管理技术应用

灾备监控与管理技术是保障灾备体系可靠运行的关键技术，需构建全方位的灾备监控与管理平台，实现对灾备系统、备份数据和恢复流程的实时监控和管理。一是灾备监控技术，通过部署监控软件和硬件设备，对主备系统的运行状态、数据同步情况、网络链路状态、存储设备状态等进行 24 小时实时监控，及时发现异常情况并发出告警。常用的监控技术包括系统监控、网络监控、存储监控、数据同步监控等。例如，采用系统监控软件，实时监控主备服务器的 CPU 利用率、内存占用率、磁盘空间等指标；采用数据同步监控技术，实时监控主备系统的数据同步延迟和同步状态。

二是灾备管理技术，通过构建灾备管理平台，实现对备份策略、备份任务、恢复流程、灾备资源的集中管理。常用的管理技术包括备份策略管理、备份任务调度、恢复流程自动化、灾备资源管理等。例如，采用备份策略管理技术，根据业务需求制定和调整备份策略；采用备份任务调度技术，自动执行全量备份、增量备份等备份任务；采用恢复流程自动化技术，实现数据恢复流程的自动化执行，提升恢复效率。

（四）灾备恢复策略制定与实施

1. 业务系统分级与恢复优先级制定

结合医院业务实际，对所有信息化业务系统进行分级，明确各系统的恢复优先级、恢复时间目标（RTO）和数据恢复点目标（RPO），为灾备策略制定提供依据。根据业务系统对医疗服务的重要程度，将业务系统划分为四级：一级系统

（核心关键业务）、二级系统（重要业务）、三级系统（一般业务）、四级系统（辅助业务）。

一级系统（核心关键业务）：指直接关系患者生命健康和医院核心运营的业务系统，包括急诊系统、重症监护系统、手术麻醉系统、HIS 核心模块（挂号、收费、住院管理）、电子病历系统。该类系统的恢复优先级最高，RTO 要求控制在 1 小时以内，RPO 要求控制在 5 分钟以内，需采用 4 级（异地热备）灾备方案。

二级系统（重要业务）：指支撑常规医疗服务和医院管理的业务系统，包括 LIS（检验信息系统）、PACS（影像归档和通信系统）、病理信息系统、药房管理系统、体检管理系统。该类系统的恢复优先级次之，RTO 要求控制在 4 小时以内，RPO 要求控制在 30 分钟以内，需采用 3 级（异地冷备）或 4 级（异地热备）灾备方案。

三级系统（一般业务）：指支撑医院辅助医疗服务和行政管理的业务系统，包括医院官网、图书馆管理系统、后勤管理系统、财务辅助系统。该类系统的恢复优先级较低，RTO 要求控制在 24 小时以内，RPO 要求控制在 2 小时以内，需采用 2 级（本地热备）或 3 级（异地冷备）灾备方案。

四级系统（辅助业务）：指医院内部的辅助办公系统，包括内部通知发布系统、考勤管理系统、员工培训系统。该类系统的恢复优先级最低，RTO 要求控制在 72 小时以内，RPO 要求控制在 24 小时以内，可采用 1 级（本地数据备份）灾备方案。

2. 灾备策略制定

根据业务系统分级结果和灾备体系分级标准，制定差异化的灾备策略，明确各业务系统的备份方式、备份频率、数据同步方式、灾备级别、恢复流程等。一是核心关键业务系统（一级系统）灾备策略：采用 4 级（异地热备）灾备方案，核心数据采用“实时同步复制 + 每日全量备份 + 每小时增量备份”的方式；主备系统采用异步复制技术，数据同步延迟控制在 5 秒以内；配置自动切换系统，主系统发生故障时自动切换到异地灾备中心，RTO 控制在 1 小时以内，RPO 控制在 5 分钟以内；定期开展主备切换测试，每季度至少开展一次，确保切换流程顺畅。

二是重要业务系统（二级系统）灾备策略：采用 3 级（异地冷备）或 4 级（异

地热备)灾备方案,核心数据采用“每日全量备份+每30分钟增量备份”的方式;采用异步复制技术将数据定时同步到异地灾备中心,数据同步频率为每30分钟一次;主系统发生故障时,采用手动或自动切换方式切换到备用系统,RTO控制在4小时以内,RPO控制在30分钟以内;每半年至少开展一次异地数据恢复测试,确保备份数据可用。

三是**一般业务系统(三级系统)灾备策略**:采用2级(本地热备)或3级(异地冷备)灾备方案,核心数据采用“每日全量备份+每2小时增量备份”的方式;本地热备系统采用同步复制技术,数据实时同步;异地冷备数据采用定时同步方式,数据同步频率为每日一次;主系统发生故障时,手动切换到备用系统或从异地备份恢复数据,RTO控制在24小时以内,RPO控制在2小时以内;每年至少开展一次数据恢复测试,确保备份数据完整。

四是**辅助业务系统(四级系统)灾备策略**:采用1级(本地数据备份)灾备方案,核心数据采用“每日全量备份”的方式;备份数据存储在本地铁带库中,加密保管;主系统发生故障时,从本地备份恢复数据,RTO控制在72小时以内,RPO控制在24小时以内;每年至少开展一次备份数据恢复测试,确保备份数据可用。

3. 灾备策略实施流程

灾备策略实施需遵循“规划设计—基础设施建设—技术部署—测试验证—运维管理”的标准化流程,确保灾备体系建设规范、可靠。一是**规划设计阶段**:结合医院业务需求和灾备策略,制定灾备体系建设规划,明确灾备机房选址、基础设施配置、技术方案选择、设备选型、实施进度和预算;组织专家对规划方案进行评审,确保方案的可行性和科学性。

二是**基础设施建设阶段**:根据规划方案,建设异地灾备机房,配备独立的电力系统(UPS电源、应急发电机)、空调系统、消防系统、安防系统等基础设施;搭建灾备网络架构,部署路由器、交换机、防火墙等网络设备,建立主备机房之间的加密通信链路;部署服务器、存储设备等硬件设备,确保硬件设备性能满足灾备需求。

三是**技术部署阶段**:根据灾备策略,部署数据备份软件、数据同步软件、自动切换软件等技术软件;配置备份策略和数据同步策略,实现核心数据的自动备份和同步;部署灾备监控与管理平台,实现对灾备系统的实时监控和管理;对主

备系统进行联调测试，确保系统运行正常。

四是测试验证阶段：开展灾备系统测试，包括数据备份测试、数据同步测试、业务切换测试、数据恢复测试等；模拟不同类型的灾难场景（如系统故障、网络瘫痪、自然灾害），检验灾备系统的响应能力和恢复效果；根据测试结果，优化灾备策略和技术方案，确保灾备系统满足业务恢复需求。

第十章 新一代通信技术引领的现代医院 信息化发展趋势与展望

第一节 6G 通信技术在医疗领域的应用前景

6G 通信技术作为新一代移动通信技术的核心,并非简单延续 5G 的技术路径,而是通过融合太赫兹通信、空天地一体化网络、人工智能内生赋能、通感算一体化等前沿技术,构建起“连接万物、智能感知、全域协同”的通信网络体系。其峰值速率可达 100Tbps、端到端时延低至 0.1 毫秒、每平方公里连接数突破 1000 万,同时具备超高可靠性(99.9999%)和全域无缝覆盖能力。这些核心特性与医疗领域对实时性、精准性、安全性、广覆盖的高要求高度契合,将在远程精准医疗、应急医疗救援、智能诊疗辅助、公共卫生防控等多个领域释放巨大应用价值,推动医疗服务从“被动响应”向“主动预判”、从“局部服务”向“全域覆盖”、从“经验驱动”向“智能精准”转型。

一、远程精准手术与微创诊疗领域的革命性突破

远程手术是医疗领域对通信技术要求最高的应用场景之一,其需要在保证手术操作实时传输的同时,确保手术器械的精准控制,任何时延或信号波动都可能引发严重医疗风险。5G 技术虽实现了远程手术的初步探索,但在时延稳定性、信号覆盖范围等方面仍存在局限,难以满足复杂微创手术的需求。6G 技术的亚毫秒级时延和超高可靠性,将彻底突破这一技术瓶颈,推动远程精准手术从“试验性应用”走向“常态化开展”。

(一) 亚毫秒级时延支撑远程精细手术操作

6G 技术通过太赫兹通信技术的应用,可实现 100Tbps 的峰值速率和 0.1 毫秒的端到端时延,远优于 5G 的 1 毫秒时延水平。这一特性使得外科医生通过远程操控手术机器人时,操作指令与机器人响应之间的延迟几乎可以忽略不计,实现“人镜合一”的操作体验。例如,在颅内微创手术、眼科精微手术等对操作精

度要求极高的场景中,6G 网络可实时传输手术区域的 4K/8K 超高清影像、手术器械的力反馈数据,医生通过 VR/AR 设备获得沉浸式手术视野,精准控制手术器械完成切割、缝合、止血等精细操作。此外,6G 的超高可靠性可确保手术过程中通信链路的持续稳定,避免因信号中断或波动导致手术中断,保障手术安全。

(二) 空天地一体化网络覆盖偏远地区远程医疗

我国地域辽阔,偏远山区、高原、海岛等地区医疗资源匮乏,且地面通信网络覆盖薄弱,难以开展常规远程医疗服务。6G 构建的空天地一体化网络,通过低轨卫星星座、高空无人机平台与地面通信网络的协同融合,可实现全域无缝覆盖,将优质医疗资源延伸至偏远地区。在偏远地区发生急重症患者需要手术时,可通过 6G 卫星通信链路,连接城市三甲医院的专家与当地医院的手术机器人,开展远程手术救治。同时,空天地一体化网络还可实时传输患者的生命体征数据、影像学检查结果等,为专家提供全面的诊疗信息,确保手术方案的科学性与精准性。例如,在高原地区发生急性心肌梗死患者需要紧急支架植入手术时,当地医院可通过 6G 网络对接省会城市心血管病专家,专家远程操控手术机器人完成手术,大幅缩短救治时间,提升救治成功率。

(三) 多模态数据融合赋能手术精准决策

6G 技术的千亿级连接密度可支持手术过程中多类医疗设备的同步接入与数据实时传输,实现手术影像、生命体征、病理数据、基因数据等多模态数据的融合分析。通过与人工智能技术的结合,可构建实时手术决策辅助系统,为医生提供精准的手术指导。例如,在肿瘤切除手术中,6G 网络可同步传输手术区域的高清影像、肿瘤的病理分型数据、患者的基因检测结果等,人工智能系统实时分析这些数据,精准定位肿瘤边界,识别周围的血管、神经等关键组织,为医生提供手术路径规划建议,避免损伤正常组织,提升手术的精准性与安全性。此外,多模态数据的实时融合还可实现手术效果的实时评估,医生可根据评估结果及时调整手术方案,提高手术成功率。

二、应急医疗救援领域的全域协同与高效处置

在突发公共卫生事件(如重大传染病疫情、突发灾害事故)应急救援中,医疗资源的快速调配、患者信息的实时共享、多部门的协同联动是提升救援效率的关键。6G 技术的全域覆盖、高速传输、低时延响应特性,可构建“全域感知、

实时协同、精准救援”的应急医疗救援体系，实现从灾害预警、伤员搜救、现场救治到后方转运的全流程高效处置。

（一）灾害现场的实时感知与伤员定位

6G 技术融合通感算一体化能力，可实现对灾害现场的精准感知与伤员的快速定位。通过部署在灾害现场的无人机、传感器网络，6G 网络可实时传输现场的图像、视频、环境数据（如温度、气压、有毒气体浓度等），为救援人员提供全面的现场态势信息。同时，基于 6G 的高精度定位技术（定位精度可达厘米级），可快速定位被困伤员的位置，尤其是在建筑坍塌、地震废墟等复杂环境中，大幅提升搜救效率。例如，在地震灾害发生后，无人机携带 6G 通信模块与高清摄像头，对灾害区域进行全方位巡查，实时传输废墟图像，通过人工智能图像识别技术快速识别被困人员；同时，伤员携带的可穿戴设备通过 6G 网络实时传输生命体征数据，救援人员可根据定位信息与生命体征数据，优先救援生命垂危的伤员。

（二）现场救治与后方专家的实时协同

在突发灾害事故现场，往往存在伤员数量多、伤情复杂、现场医疗资源不足的问题，需要后方专家的实时指导。6G 技术的高速率、低时延特性，可实现现场救治与后方专家的实时协同。现场医护人员通过便携式医疗设备采集伤员的生命体征数据、影像学检查结果（如便携式 CT、超声检查数据），通过 6G 网络实时传输给后方医院的专家；专家通过 VR/AR 设备获得现场的沉浸式视野，实时指导现场医护人员开展救治工作，如创伤止血、骨折固定、气道管理等。此外，6G 网络还可支持多学科专家的同步会诊，针对复杂伤情快速制定救治方案，提升现场救治的专业性与规范性。例如，在重大交通事故现场，多名伤员出现复合伤，现场医护人员通过 6G 网络连接骨科、胸外科、神经外科等多学科专家，专家同步会诊制定个性化救治方案，指导现场开展紧急救治。

（三）跨区域医疗资源的快速调配与转运协同

突发公共卫生事件中，跨区域医疗资源的快速调配与伤员的高效转运是保障救治效果的重要环节。6G 技术构建的全域协同网络，可实现医疗资源信息的实时共享与转运过程的全程监控。通过 6G 网络，可实时汇总各地医院的床位资源、医疗设备资源、医护人员资源等信息，构建全国性的医疗资源调度平台，根据灾害现场的伤员数量与伤情分布，精准调配医疗资源。在伤员转运过程中，救护车通过 6G 网络实时传输伤员的生命体征数据、转运轨迹等信息，后方医院可提前

做好救治准备，如预留床位、调配医护人员、准备手术设备等；同时，6G 网络可支持救护车与空中救援直升机的协同调度，实现“空地一体化”转运，大幅缩短转运时间。例如，在重大传染病疫情爆发时，通过 6G 医疗资源调度平台，可快速调配各地的呼吸机、防护服等医疗物资到疫情严重地区，同时协调各地医院接收轻症患者，实现医疗资源的优化配置。

三、智能诊疗辅助与个性化医疗领域的深度赋能

随着精准医疗理念的普及，个性化诊疗已成为医疗发展的重要方向，其需要基于患者的基因数据、病理数据、生活习惯等多维度信息，制定个性化的诊疗方案。6G 技术的高速数据传输、海量连接与人工智能内生赋能特性，可推动智能诊疗辅助系统的升级与完善，实现从疾病筛查、诊断到治疗、康复的全流程个性化医疗服务。

（一）海量医疗数据的实时分析与精准诊断

医疗领域产生的海量数据（如电子病历、影像数据、基因测序数据、wearable 设备数据等）是实现精准诊断的基础，但这些数据具有体量大、类型多、增长快的特点，传统通信技术难以实现实时传输与高效分析。6G 技术的 100Tbps 峰值速率可实现海量医疗数据的秒级传输，结合边缘计算与云计算的协同，可实现医疗数据的实时分析与处理。例如，在基因测序领域，人类全基因组测序数据量可达 100GB 以上，通过 6G 网络可将测序数据实时传输至边缘计算节点，结合人工智能算法快速分析基因变异位点，为肿瘤、遗传病等疾病的诊断提供精准依据；在影像诊断领域，6G 网络可实时传输患者的 CT、MRI 等影像数据，人工智能影像诊断系统快速识别病灶，为医生提供诊断建议，提升诊断效率与准确性。此外，6G 技术还可支持多中心医疗数据的协同分析，打破医院之间的数据壁垒，构建大规模医疗数据共享平台，提升人工智能诊断模型的泛化能力。^①

（二）可穿戴设备与植入式医疗设备的全域连接

可穿戴设备（如智能手环、动态血糖监测仪、心电监测背心等）与植入式医疗设备（如心脏起搏器、人工耳蜗、脑机接口设备等）是实现个性化医疗与慢病管理的重要载体。6G 技术的千亿级连接密度可支持海量可穿戴设备与植入式医

① 杨建强. 智慧医院建设背景下会计信息化转型实施策略分析 [J]. 行政事业资产与财务, 2025, (21): 64-66.

疗设备的同时接入,实现患者生命体征数据的实时采集与传输。例如,糖尿病患者佩戴的动态血糖监测仪,通过 6G 网络可实时将血糖数据传输至医生的诊疗平台,医生根据血糖数据变化及时调整用药方案;心脏起搏器植入患者的心率、心律数据通过 6G 网络实时传输,一旦出现异常,系统可自动发出告警,医生可远程指导患者进行应急处理,甚至远程调整起搏器参数。此外,6G 技术的低功耗特性可延长植入式医疗设备的续航时间,减少患者的手术更换次数,提升患者的生活质量。

（三）个性化治疗方案的实时优化与康复指导

6G 技术结合人工智能与虚拟现实技术,可实现个性化治疗方案的实时优化与康复过程的精准指导。在肿瘤治疗领域,通过 6G 网络实时传输患者的治疗反应数据(如肿瘤大小变化、血常规数据等),人工智能系统结合患者的基因数据与治疗历史,实时优化放疗、化疗方案,提升治疗效果;在康复治疗领域,患者佩戴的可穿戴设备通过 6G 网络实时传输运动姿态数据,医生通过 VR 设备远程观察患者的康复训练情况,实时纠正训练动作,制定个性化的康复训练计划。例如,脑卒中患者的康复过程中,可穿戴设备采集患者的肢体运动数据,通过 6G 网络传输至康复指导平台,人工智能系统分析运动数据与康复目标的差距,为患者推送个性化的康复训练视频,医生通过 VR 设备实时指导患者训练,提升康复效果。

四、公共卫生防控领域的智能化与精细化升级

公共卫生防控的核心是实现疫情的早期预警、快速响应与精准管控。6G 技术的全域感知、高速传输与大数据分析能力,可推动公共卫生防控体系从“被动应对”向“主动预警”转型,实现疫情的早发现、早报告、早隔离、早治疗。

（一）疫情的早期预警与风险预判

6G 技术融合多源数据采集与人工智能分析,可实现疫情的早期预警与风险预判。通过部署在公共场所(如机场、火车站、商场等)的智能监测设备(如红外测温仪、人脸识别设备、环境病毒检测传感器等),6G 网络可实时采集人员流动数据、体温数据、环境病毒浓度数据等多维度信息;结合大数据分析 with 人工智能算法,可快速识别疫情传播的潜在风险点,如人员聚集区域、病毒传播链等,提前发出预警。例如,在流感疫情高发期,通过 6G 网络采集各地的流感样病例数据、环境温湿度数据、人员流动数据等,人工智能系统可预测流感疫情的传播

趋势，为公共卫生部门制定防控策略提供依据；在新发传染病疫情早期，通过环境病毒检测传感器实时采集数据，结合基因测序数据的快速传输与分析，可快速识别新型病毒，为疫情防控争取时间。

（二）疫情的精准管控与资源调度

在疫情爆发后，6G 技术可实现疫情的精准管控与医疗资源的高效调度。通过 6G 网络的高精度定位与人员流动轨迹追踪，可快速锁定密切接触者，实现精准隔离；同时，实时汇总各地的疫情数据（如确诊病例数量、疑似病例数量、医疗资源占用情况等），构建疫情防控指挥平台，公共卫生部门可根据疫情数据实时调整防控策略，调配医疗资源。例如，在新冠疫情防控中，通过 6G 网络追踪确诊病例的活动轨迹，快速排查密切接触者并推送隔离通知；同时，疫情防控指挥平台可实时监控各地医院的床位资源、呼吸机资源等，精准调配医疗资源到疫情严重地区，提升防控效果。

（三）疫苗研发与防控科普的高效推进

6G 技术可加速疫苗研发进程，同时推动防控科普的广泛传播。在疫苗研发领域，通过 6G 网络实现多中心疫苗临床试验数据的实时共享与协同分析，可加快疫苗研发的速度；结合人工智能算法，可快速筛选疫苗候选靶点，优化疫苗配方。在防控科普领域，6G 技术支持超高清视频、VR/AR 等沉浸式科普内容的实时传输，可通过手机、智能电视、VR 设备等多种终端，向公众普及疫情防控知识，提升公众的防控意识与能力。例如，通过 VR 设备为公众模拟疫情传播场景，让公众直观了解病毒传播途径与防控措施；通过超高清视频实时直播疫苗接种过程，解答公众的疑问，提升疫苗接种率。

五、6G 医疗应用的挑战与应对策略

尽管 6G 技术在医疗领域具有广阔的应用前景，但要实现规模化落地，仍面临技术、安全、伦理、成本等多方面的挑战，需要政府、企业、医院等多方协同应对。

（一）核心技术瓶颈与突破路径

6G 技术的发展仍面临太赫兹通信技术成熟度不足、空天地一体化网络协同难度大、核心芯片与元器件国产化率低等技术瓶颈。针对这些问题，需要加强产学研协同创新，加大核心技术研发投入。一方面，聚焦太赫兹通信、空天地一体

化网络、核心芯片等关键技术领域,组建专项研发团队,突破技术瓶颈;另一方面,推动 6G 技术与医疗领域的深度融合,开展针对性的技术研发与应用试点,如远程手术专用通信设备、医疗数据安全传输技术等,提升技术的实用性与成熟度。

（二）数据安全与隐私保护风险

6G 技术在实现海量医疗数据实时传输与共享的同时,也带来了数据安全与隐私保护的风险,如医疗数据泄露、篡改、滥用等。为应对这些风险,需要构建全方位的医疗数据安全保障体系。一是加强数据加密技术的应用,采用端到端加密、区块链等技术,确保医疗数据在传输、存储、使用过程中的安全性;二是完善相关法律法规与管理制度,明确医疗数据的所有权、使用权与保护责任,规范医疗数据的采集、传输、共享流程;三是加强数据安全监管,建立医疗数据安全监测平台,实时监测数据异常访问行为,及时发现并处置安全风险。

（三）伦理与法律争议

6G 医疗应用还面临一系列伦理与法律争议,如远程手术的责任认定、人工智能诊断的伦理边界、植入式医疗设备的隐私保护等。针对这些问题,需要加快完善相关伦理规范与法律法规。一方面,制定 6G 医疗应用的伦理准则,明确技术应用的边界与责任划分,如远程手术中医生、医院、通信运营商的责任认定;另一方面,修订完善现有法律法规,将 6G 医疗应用纳入监管范围,规范技术应用的审批流程与操作标准,保障患者的合法权益。

（四）建设成本与资源整合难题

6G 网络建设与医疗应用落地需要巨额的资金投入,包括基站建设、卫星星座部署、医疗设备升级等,同时还面临医疗资源与通信资源整合难度大的问题。为解决这些问题,需要政府、企业、医院多方协同发力。政府层面,加大政策支持与资金投入,出台相关补贴政策,引导社会资本参与 6G 医疗应用建设;企业层面,加强通信企业与医疗企业的合作,共同研发 6G 医疗专用设备与解决方案,降低应用成本;医院层面,推进信息化建设升级,加强医疗数据标准化建设,提升与 6G 网络的适配性。

第二节 新一代通信技术驱动的智慧医院建设的发展方向

新一代通信技术（5G-A、6G）的发展与应用，正推动智慧医院建设进入全新的发展阶段。智慧医院建设不再局限于单个医院的信息化升级，而是朝着全域协同、精准智能、普惠可及、绿色低碳的方向发展，构建“以患者为中心”的全周期医疗服务体系。依托新一代通信技术的支撑，智慧医院将实现医疗服务、管理、教学、科研等全领域的升级，推动医疗资源的优化配置，提升医疗服务效率与质量，满足人民群众日益增长的医疗健康需求。

一、全域协同医疗服务体系的构建

新一代通信技术的全域覆盖与高速协同特性，将打破医院之间、区域之间的信息壁垒，推动构建“区域协同、城乡一体、上下联动”的全域协同医疗服务体系，实现医疗资源的优化配置与医疗服务的同质化。

（一）区域医疗协同网络的升级与完善

基于 5G-A、6G 技术，将构建更加高效、稳定的区域医疗协同网络，实现区域内各级医院的信息实时共享与业务协同。通过区域医疗协同平台，可实现电子病历、影像数据、检验结果等医疗信息的跨医院共享，避免患者重复检查，提升诊疗效率；同时，可开展远程会诊、远程门诊、远程检查等协同医疗服务，让基层医院的患者能够享受到上级医院的优质医疗资源。例如，在县域医共体建设中，通过 6G 区域医疗协同网络，县级医院可与乡镇卫生院实现医疗信息实时共享，县级医院专家可远程指导乡镇卫生院医生开展诊疗工作，提升基层医疗服务水平；同时，乡镇卫生院的疑难病例可快速转诊至县级医院，实现“小病不出乡、大病不出县”的诊疗目标。

（二）跨区域医疗资源的精准调配与协同救治

新一代通信技术将推动跨区域医疗资源的精准调配与协同救治，提升重大疾病与突发公共卫生事件的救治能力。通过构建全国性的医疗资源调度平台，基于 6G 网络的实时数据传输与分析，可实时汇总各地医疗资源信息（如床位、设备、医护人员）与患者需求信息，实现医疗资源的跨区域精准调配。在重大疾病救治中，如疑难肿瘤、罕见病等，可通过跨区域多学科会诊平台，组织全国顶尖专家开展协同会诊，制定个性化救治方案；在突发公共卫生事件中，可快速协调各地

医疗资源支援疫情严重地区，实现跨区域协同防控与救治。例如，在全国范围内构建肿瘤诊疗协同网络，通过 6G 网络实现肿瘤患者的影像数据、病理数据、基因数据等跨医院共享，组织不同地区的肿瘤专家开展协同会诊，为患者制定最优治疗方案。

（三）城乡医疗资源的均衡配置与下沉

新一代通信技术将有效破解城乡医疗资源不均衡的难题，推动优质医疗资源下沉到基层。通过 6G 空天地一体化网络，可将城市三甲医院的优质医疗资源延伸至偏远农村地区，开展远程诊疗、远程培训等服务；同时，通过智能诊疗设备与可穿戴设备的部署，可实现基层医疗机构的智能化升级，提升基层医疗服务能力。例如，为偏远农村地区的村卫生室配备智能诊疗终端与 6G 通信模块，村民可通过终端实现远程挂号、远程问诊、远程检查等服务，城市专家可实时查看村民的健康数据，提供诊疗建议；同时，通过 6G 网络为基层医生提供远程培训，提升基层医生的专业水平。此外，还可通过“互联网+医疗”模式，开展药品配送、健康管理等服务，提升农村地区医疗服务的可及性。

二、精准智能诊疗模式的全面升级

新一代通信技术与人工智能、大数据、物联网等技术的深度融合，将推动诊疗模式从“经验驱动”向“精准智能驱动”升级，实现疾病的早发现、早诊断、早治疗，提升诊疗效果与患者体验。

（一）智能问诊与预诊断系统的普及应用

基于新一代通信技术的高速传输与人工智能技术的升级，智能问诊与预诊断系统将在智慧医院中广泛应用。患者通过手机、智能终端等渠道，可与智能问诊系统进行实时交互，系统通过分析患者的症状描述、病史信息、生活习惯等数据，快速给出预诊断建议与就诊指导，引导患者精准挂号，避免盲目就医。同时，智能问诊系统可将患者的预诊断信息与健康数据实时传输至医院诊疗平台，医生在接诊前可提前了解患者情况，提升诊疗效率。例如，患者出现咳嗽、发烧等症状时，通过智能问诊系统描述症状后，系统结合实时采集的体温、心率等数据，初步判断可能的疾病类型，推荐对应的科室与医生，并提醒患者携带相关病历资料，大幅缩短患者的就诊时间。

（二）人工智能辅助诊断技术的深度应用

新一代通信技术的高速数据传输能力，将推动人工智能辅助诊断技术在影像诊断、病理诊断、实验室诊断等领域的深度应用。通过 6G 网络，可实现海量影像数据、病理切片数据、实验室检测数据的实时传输与分析，人工智能辅助诊断系统可快速识别病灶、分析检测结果，为医生提供精准的诊断建议，提升诊断的准确性与效率。例如，在影像诊断领域，人工智能系统通过 6G 网络实时分析患者的 CT、MRI 影像，快速识别肺部结节、肿瘤等病灶，并标注病灶的位置、大小、形态等信息，为放射科医生提供诊断参考；在病理诊断领域，人工智能系统可快速分析病理切片，识别癌细胞、异常组织等，辅助病理医生做出准确诊断。此外，人工智能辅助诊断技术还可实现多模态数据的融合分析，提升复杂疾病的诊断能力。

（三）个性化治疗与精准康复的智能化推进

新一代通信技术将推动个性化治疗与精准康复的智能化发展，实现从治疗到康复的全流程精准管理。在个性化治疗方面，通过 6G 网络实时传输患者的基因数据、病理数据、治疗反应数据等，结合人工智能算法，可制定个性化的治疗方案，并实时优化治疗策略；同时，可通过智能医疗设备实现治疗过程的精准控制，如智能输液系统根据患者的体重、病情等数据自动调节输液速度，智能放疗设备精准定位肿瘤组织，提升治疗效果。在精准康复方面，通过可穿戴设备实时采集患者的运动数据、生命体征数据，通过 6G 网络传输至康复管理平台，人工智能系统分析患者的康复进展，制定个性化的康复训练计划，医生通过 VR 设备远程指导患者开展康复训练，提升康复效果。例如，脑卒中患者的康复过程中，可穿戴设备采集患者的肢体运动数据，通过 6G 网络传输至康复平台，系统根据数据调整康复训练强度与内容，医生通过 VR 设备实时纠正患者的训练动作，加快患者康复。

三、全周期健康管理体的构建

新一代通信技术将推动智慧医院从“疾病治疗”向“全周期健康管理”转型，构建覆盖预防、诊疗、康复、养老等全环节的健康管理体系，实现对患者的全生命周期健康服务。

（一）精准预防与健康监测体系的完善

基于新一代通信技术与可穿戴设备、智能传感器的融合，将构建精准预防与健康监测体系，实现疾病的早期预警与预防。通过可穿戴设备实时采集居民的生命体征数据（如心率、血压、血糖、睡眠等），通过 6G 网络传输至健康管理平台，人工智能系统分析数据变化趋势，识别潜在的健康风险，提前发出预警并推送个性化的预防建议。例如，高血压患者佩戴的智能血压监测仪，通过 6G 网络实时传输血压数据，系统发现血压异常升高时，及时向患者与医生发出预警，医生指导患者调整饮食、运动与用药方案，预防并发症的发生；对于健康人群，系统根据其生活习惯、体检数据等，推送个性化的健康管理建议，如运动计划、饮食指导等，提升居民的健康意识与自我管理能力。

（二）诊疗与康复的全流程协同管理

新一代通信技术将实现诊疗与康复的全流程协同管理，提升医疗服务的连续性与有效性。在诊疗过程中，医生通过智慧诊疗平台可实时查看患者的健康数据、诊疗记录等，制定个性化的诊疗方案；在康复过程中，康复医生可通过 6G 网络实时监控患者的康复训练情况，及时调整康复计划，实现诊疗与康复的无缝衔接。同时，通过健康管理平台，可实现患者与医生的实时沟通，患者可随时咨询康复过程中的问题，医生及时给出指导建议，提升康复效果。例如，骨科手术后患者的康复过程中，医生通过 6G 网络实时查看患者的康复训练数据与伤口愈合情况，调整康复训练计划，患者通过手机终端随时向医生反馈康复进展，实现诊疗与康复的全流程协同。

（三）医养结合与老年健康管理的智能化发展

随着人口老龄化的加剧，医养结合已成为养老服务的重要发展方向。新一代通信技术将推动医养结合与老年健康管理的智能化发展，提升老年人群的健康服务水平。通过在养老机构、社区养老服务中心部署智能监测设备、紧急呼叫系统等，通过 6G 网络实现老年人心率、血压等生命体征数据的实时监测与紧急情况的快速响应；同时，通过远程诊疗、远程护理等服务，让老年人足不出户就能享受到优质的医疗服务。例如，在养老机构中，老年人佩戴的智能手环实时传输生命体征数据，一旦出现异常，系统自动发出告警，养老机构工作人员与医院医生可及时响应；同时，医生通过远程视频为老年人开展定期体检、慢病管理等服务，提升老年人的生活质量。此外，还可通过 VR 技术为老年人提供心理健康服务，如心理疏导、娱乐活动等，缓解老年人的孤独感。

四、智慧医院管理与运营的精细化升级

新一代通信技术将推动智慧医院管理与运营的精细化升级，提升医院的管理效率、运营效益与服务质量，实现医院的可持续发展。

（一）医院资源的智能化调度与管理

基于新一代通信技术与物联网、大数据技术的融合，将实现医院资源的智能化调度与管理，提升资源利用效率。通过在医院内部部署智能传感器、射频识别（RFID）设备等，实时采集医疗设备、药品、床位、医护人员等资源的信息，通过 6G 网络传输至医院资源管理平台，系统根据资源使用情况与患者需求，实现资源的智能调度。例如，医院的智能药房通过 6G 网络实时接收处方信息，自动调配药品，减少患者取药等待时间；智能床位管理系统实时监控床位使用情况，根据患者病情与诊疗需求，智能分配床位，提升床位利用率；医护人员定位系统通过 6G 网络实时追踪医护人员位置，在紧急情况下快速调配医护人员，提升应急响应效率。

（二）医院运营成本的精准管控

新一代通信技术将推动医院运营成本的精准管控，降低运营成本，提升运营效益。通过大数据分析与人工智能技术，对医院的人力成本、物资成本、能耗成本等进行实时监控与分析，识别成本管控的关键点，制定个性化的成本管控方案。例如，通过智能能耗监测系统，实时采集医院的水电油气等能耗数据，通过 6G 网络传输至能耗管理平台，系统分析能耗数据变化趋势，识别能耗浪费点，推送节能建议，降低医院能耗成本；通过物资管理系统，实时监控药品、耗材等物资的库存情况，实现物资的精准采购与管理，减少物资浪费与积压。此外，还可通过智能化的财务管理系统，实现医院财务数据的实时分析与精准核算，提升财务管理效率。

（三）医院服务质量的智能化评估与提升

新一代通信技术将推动医院服务质量的智能化评估与提升，提升患者满意度。通过在医院内部部署智能评价设备、满意度调查系统等，实时采集患者的服务评价数据，通过 6G 网络传输至服务质量评估平台，系统分析患者评价数据，识别服务质量存在的问题，推送改进建议；同时，通过视频监控、智能语音分析等技术，实时监控医护人员的服务态度、诊疗行为等，规范医护人员的服务流程，提

升服务质量。例如，患者在就诊结束后，通过手机终端或医院自助设备对诊疗服务进行评价，系统实时分析评价数据，对于患者反映的问题，及时反馈给相关科室并督促整改；通过智能语音分析系统，分析医护人员与患者的沟通记录，规范沟通语言与服务流程，提升患者的就医体验。

五、医学教育与科研的数字化转型

新一代通信技术将推动医学教育与科研的数字化转型，提升医学人才培养质量与科研创新能力，为智慧医院建设提供人才与技术支撑。

（一）医学教育的智能化与沉浸式发展

基于新一代通信技术与 VR/AR、元宇宙等技术的融合，将推动医学教育的智能化与沉浸式发展，提升医学人才培养质量。通过 6G 网络传输超高清医学教学视频、VR/AR 教学内容，医学生可通过 VR 设备开展沉浸式临床技能训练，如模拟手术、模拟问诊等，提升实践操作能力；同时，可通过远程教学平台，实现优质医学教育资源的跨区域共享，让偏远地区的医学生也能享受到顶尖的医学教育资源。例如，医学生通过 VR 设备模拟颅内微创手术，通过 6G 网络实时传输操作数据，教师可远程指导学生的操作动作，纠正错误，提升手术技能；通过元宇宙医学教育平台，医学生可与虚拟患者进行交互，模拟不同疾病的诊疗过程，提升临床诊疗能力。

（二）医学科研的协同化与智能化升级

新一代通信技术将推动医学科研的协同化与智能化升级，提升科研创新能力。通过 6G 网络构建多中心科研协同平台，实现科研数据的实时共享与协同分析，加快科研项目的推进速度；结合人工智能技术，可实现科研数据的快速分析与挖掘，发现疾病的发病机制、治疗靶点等，提升科研效率。例如，在肿瘤科研领域，通过多中心科研协同平台，实现不同医院的肿瘤患者数据、样本数据的实时共享，结合人工智能算法快速分析数据，发现肿瘤的基因变异规律与治疗靶点，加快肿瘤新药与新治疗方案的研发；在传染病科研领域，通过 6G 网络实时采集疫情数据、病毒基因数据等，结合人工智能算法预测疫情传播趋势，为疫情防控提供科研支撑。

（三）医学知识管理与传承的数字化推进

新一代通信技术将推动医学知识管理与传承的数字化推进，实现医学知识的

高效传播与传承。通过构建数字化医学知识管理平台,整合医学文献、临床案例、诊疗指南等知识资源,通过 6G 网络实现知识资源的实时更新与共享;同时,通过人工智能技术,可实现医学知识的智能检索与推送,帮助医护人员快速获取所需的医学知识,提升诊疗水平。例如,医生在诊疗过程中遇到疑难病例时,通过医学知识管理平台快速检索相关的临床案例与诊疗指南,结合患者的具体情况制定诊疗方案;通过数字化平台,资深专家的临床经验与诊疗技巧可转化为数字化资源,传承给年轻医护人员,提升医学人才的培养质量。

六、智慧医院建设的挑战与发展建议

新一代通信技术驱动的智慧医院建设虽前景广阔,但仍面临技术融合、数据治理、人才培养、标准规范等多方面的挑战,需要政府、医院、企业等多方协同发力,推动智慧医院建设高质量发展。

(一) 核心挑战分析

一是技术融合难度大。智慧医院建设需要融合新一代通信技术、人工智能、大数据、物联网等多种技术,不同技术之间的适配性与协同性面临挑战,如 6G 网络与医疗设备的适配、医疗数据与人工智能算法的融合等。二是数据治理能力不足。医疗数据具有体量大、类型多、标准不统一的特点,数据采集、存储、传输、共享等环节的治理能力不足,影响数据的有效利用。三是专业人才匮乏。智慧医院建设需要既懂医疗又懂通信、信息技术的复合型人才,目前这类人才数量不足,难以满足智慧医院建设的需求。四是标准规范不健全。智慧医院建设涉及的技术应用、数据共享、服务流程等方面的标准规范不健全,导致不同医院、不同区域之间的智慧医疗系统难以互联互通。五是资金投入压力大。智慧医院建设需要巨额的资金投入,包括网络建设、设备升级、人才培养等,医院的资金投入压力较大。

(二) 发展建议

一是加强技术创新。政府应加大对智慧医疗技术融合创新的支持力度,鼓励通信企业、医疗企业、科研机构开展协同创新,突破技术融合瓶颈,研发适配智慧医院建设的核心技术与解决方案;医院应积极推进信息化建设升级,提升医疗设备与信息系统的技术适配性,推动技术与医疗业务的深度融合。二是提升数据治理能力。建立健全医疗数据标准规范,推动医疗数据的标准化采集与管理;

加强医疗数据安全保障体系建设，采用加密、区块链等技术确保数据安全；构建医疗数据共享平台，推动跨医院、跨区域医疗数据的有序共享与有效利用。三是加强专业人才培养。高校应优化医学教育专业设置，增设智慧医疗相关专业，培养复合型人才；医院应加强对现有医护人员的信息技术培训，提升其智慧医疗技术应用能力；企业应加强对技术人员的医疗知识培训，提升其技术研发的针对性与实用性。四是完善标准规范体系。政府应牵头制定智慧医院建设的相关标准规范，包括技术应用标准、数据共享标准、服务流程标准等，规范智慧医院建设与运营；推动行业协会、企业、医院参与标准规范的制定与推广，确保标准规范的科学性与实用性。五是加大政策支持与资金投入。政府应出台相关政策，加大对智慧医院建设的资金支持，引导社会资本参与智慧医院建设；医院应优化资金配置，加大对智慧医疗技术与设备的投入，同时加强成本管控，提升资金使用效益。

第三节 新一代通信技术应用的政策支持与行业标准化建设

新一代通信技术与医疗健康领域的深度融合，离不开政策的顶层设计与精准引导，也依赖于行业标准的统一规范与协同推进。近年来，国家层面、行业主管部门及地方政府纷纷出台一系列政策文件，从战略规划、资金支持、试点示范等多维度为新一代通信技术在医疗领域的应用保驾护航；同时，行业协会、科研机构与龙头企业协同发力，在技术应用、数据共享、安全保障等关键领域推进标准化建设，为新一代通信技术在医院信息化建设中的规模化、规范化应用奠定基础。政策支持与行业标准化建设相互促进、协同发力，共同构建起新一代通信技术驱动医院信息化发展的制度保障体系。

一、新一代通信技术医疗应用的政策支持体系构建

我国新一代通信技术医疗应用的政策支持体系呈现出“顶层规划引领、部门协同推进、地方精准落地”的多层级、全方位特征。国家层面聚焦战略定位，明确发展方向；行业主管部门细化实施路径，强化监管引导；地方政府结合区域实际，推出差异化支持政策，形成了覆盖规划、资金、技术、人才等多维度的政策保障网络，有效激发了市场主体活力，加速了新一代通信技术在医疗领域的落地应用。

（一）国家层面战略规划与顶层设计

国家层面将新一代通信技术与医疗健康的融合发展纳入重大战略规划，为行业发展指明方向。《“健康中国 2030”规划纲要》明确提出“推进健康医疗大数据应用”“发展智慧医疗”，强调要利用新一代信息技术优化医疗服务流程，提升医疗服务效率与质量。《数字中国建设整体布局规划》将“智慧健康”作为数字中国建设的重要内容，要求推动 5G、6G 等新一代通信技术与医疗健康领域深度融合，构建全域协同的智慧医疗服务体系。此外，国家“十四五”规划纲要也明确提出“加快 5G 网络规模化部署，前瞻布局 6G 网络技术储备”，并将智慧医疗作为 5G、6G 技术的重点应用场景之一，从国家战略层面确立了新一代通信技术在医疗健康领域的重要地位。^①

在政策引导的同时，国家层面还通过重大科技专项、产业基金等方式加大资金支持力度。例如，国家重点研发计划设立“数字诊疗装备研发”“主动健康与老龄化科技应对”等专项，将新一代通信技术与医疗设备的融合创新作为重点研发方向，支持科研机构与企业开展关键技术攻关；国家发改委、工信部等部门设立新一代信息基础设施建设专项基金，支持 5G、6G 基站建设及智慧医疗平台搭建，为新一代通信技术医疗应用提供基础设施保障。此外，国家还通过税收优惠、政府采购等政策，鼓励医院、通信企业、医疗设备企业等市场主体参与新一代通信技术医疗应用项目建设，降低应用成本，提升应用积极性。

（二）行业主管部门协同推进与监管引导

国家卫生健康委、工信部、科技部、国家药监局等行业主管部门建立协同推进机制，细化政策措施，强化监管引导，推动新一代通信技术医疗应用规范有序发展。卫生健康委作为医疗行业主管部门，牵头制定智慧医院建设标准、远程医疗服务规范等政策文件，明确新一代通信技术在医院信息化建设中的应用要求与评价指标；工信部聚焦通信技术与医疗设备的融合创新，推动 5G、6G 技术在医疗领域的应用试点，组织开展“5G+ 医疗健康”应用征集活动，推广优秀应用案例；科技部加强关键技术研发支持，推动产学研协同创新，突破新一代通信技术医疗应用的核心技术瓶颈；国家药监局则强化对智能医疗设备、远程诊疗设备等产品的监管，制定相关产品注册审批规范，保障医疗服务安全。

① 刘轩. 医院运营效率提升策略与问题研究 [J]. 经济师, 2025, (11): 227-228.

例如，国家卫生健康委与工信部联合印发《关于进一步加强 5G+ 医疗健康创新应用的通知》，明确提出要推进 5G 在远程医疗、应急救援、智能诊疗等领域的应用，建设一批 5G+ 医疗健康示范项目，培育一批创新企业与人才团队；联合发布《5G+ 医疗健康应用场景目录》，梳理出远程会诊、远程手术、应急救援等 10 大应用场景，为各地开展 5G+ 医疗健康应用提供指引。此外，各部门还通过建立跨部门监管机制，加强对医疗数据安全、隐私保护等方面的监管，规范新一代通信技术医疗应用的发展秩序。

（三）地方层面精准落地与差异化支持

地方政府结合区域医疗资源禀赋与信息化发展水平，出台差异化的支持政策，推动新一代通信技术医疗应用精准落地。各地纷纷将智慧医疗作为地方数字经济发展的重要抓手，通过出台专项规划、设立地方专项基金、推进试点示范项目建设等方式，加大对新一代通信技术医疗应用的支持力度。例如，广东省印发《广东省 5G+ 医疗健康应用发展行动计划》，提出到 2025 年建成一批 5G+ 医疗健康示范医院，培育一批具有核心竞争力的创新企业，形成覆盖全省的 5G+ 医疗健康服务网络；浙江省推出《浙江省智慧医院建设指南》，将 5G、人工智能等技术应用作为智慧医院建设的核心指标，支持医院开展信息化升级改造；北京市设立智慧医疗专项基金，重点支持 6G 医疗应用技术研发与试点示范，推动优质医疗资源通过新一代通信技术向郊区、偏远地区延伸。

地方政府还积极推进跨区域协同政策落地，例如，长三角地区三省一市联合出台《长三角区域 5G+ 医疗健康协同发展行动计划》，推动区域内医疗数据共享、远程医疗协同、医疗资源优化配置，实现新一代通信技术医疗应用的跨区域协同发展；成渝地区双城经济圈推出智慧医疗协同发展政策，支持两地医院通过 5G 网络开展远程会诊、联合科研等活动，提升区域医疗服务协同能力。此外，地方政府还通过优化营商环境、加强人才引育等政策，吸引通信企业、医疗设备企业等落户，构建新一代通信技术医疗应用的产业生态。

（四）政策支持体系的协同效应与实施成效

多层级的政策支持体系形成了强大的协同效应，有效推动了新一代通信技术在医疗领域的应用落地与产业发展。在政策引导下，我国 5G+ 医疗健康应用已实现全国所有地级市、县城城区覆盖，建成了一批 5G+ 远程医疗、5G+ 智能诊疗等示范项目。例如，全国已有超过 1000 家医院开展 5G+ 远程会诊服务，覆盖

偏远地区县级医院；多家三甲医院开展 5G+ 远程手术试点，成功完成颅内手术、骨科手术等复杂手术；各地建设的智慧健康管理平台，通过 5G 网络实现对慢病患者的实时监测与健康管理的。

政策支持还推动了新一代通信技术医疗应用产业生态的完善，形成了“通信企业 + 医疗设备企业 + 医院 + 科研机构”的协同创新模式。例如，华为、中兴等通信企业与迈瑞医疗、联影医疗等医疗设备企业合作，研发 5G+ 智能医疗设备；医院与科研机构联合开展新一代通信技术医疗应用临床研究，推动技术成果转化。同时，政策支持也提升了我国在新一代通信技术医疗应用领域的国际竞争力，相关技术标准与应用案例在国际上得到广泛关注与认可。

二、新一代通信技术医疗应用的行业标准化建设

行业标准化建设是新一代通信技术在医疗领域规模化、规范化应用的关键支撑。当前，我国新一代通信技术医疗应用的标准化建设正从基础通用标准向细分领域专用标准延伸，从技术应用标准向数据安全、服务质量标准拓展，形成了“国家标准引领、行业标准支撑、团体标准补充”的多元化标准体系。行业协会、科研机构、龙头企业等主体积极参与标准化制定工作，在技术接口、数据共享、安全保障、服务流程等关键领域取得一系列突破，为新一代通信技术在医院信息化建设中的应用提供了统一的技术规范与操作指南。

（一）基础通用标准体系建设

基础通用标准是新一代通信技术医疗应用标准化建设的基础，主要涵盖术语定义、技术架构、接口规范等方面。在术语定义方面，全国信息技术标准化技术委员会、国家卫生健康标准委员会联合制定《智慧医疗术语》国家标准，明确了新一代通信技术医疗应用相关术语的定义与内涵，规范了行业用语；在技术架构方面，工信部牵头制定《5G+ 医疗健康技术架构要求》行业标准，明确了 5G+ 医疗健康系统的总体架构、功能模块、技术要求等，为系统建设提供了架构指引；在接口规范方面，中国通信标准化协会制定《5G 医疗设备通信接口技术要求》，规范了 5G 医疗设备与通信网络、医院信息系统之间的接口协议，确保设备之间的互联互通。

基础通用标准的建设有效解决了新一代通信技术医疗应用中“语言不通、架构不一、接口不兼容”的问题。例如，统一的接口规范使得不同厂家生产的 5G

医疗设备能够顺畅接入医院信息系统，实现数据的实时共享与交互；统一的技术架构要求确保了各地建设的 5G+ 医疗健康平台能够遵循统一的技术路径，为后续跨区域协同奠定基础。此外，基础通用标准还为行业监管提供了依据，有助于规范市场秩序，提升行业整体发展水平。

（二）细分领域专用标准建设

随着新一代通信技术在医疗领域应用的不断深入，细分领域专用标准建设成为重点方向，涵盖远程医疗、智能诊疗、应急救援、健康管理等多个领域。在远程医疗领域，国家卫生健康委制定《远程医疗服务规范》《5G+ 远程手术技术要求》等标准，明确了远程会诊、远程手术等服务的流程、技术要求、质量控制指标等；在智能诊疗领域，中国医院协会制定《人工智能辅助诊断系统应用规范》，规范了人工智能辅助诊断系统在影像诊断、病理诊断等领域的应用流程与评价标准；在应急救援领域，工信部与国家卫生健康委联合制定《5G+ 应急医疗救援技术规范》，明确了 5G 技术在灾害现场救援、伤员转运等环节的应用要求与协同机制；在健康管理领域，中国保健协会制定《智慧健康管理平台建设标准》，规范了健康数据采集、分析、应用等环节的技术要求。

细分领域专用标准的建设提升了新一代通信技术医疗应用的针对性与可操作性。例如，《5G+ 远程手术技术要求》对手术机器人的通信延迟、数据传输速率、安全性等指标做出了明确规定，确保远程手术的安全开展；《人工智能辅助诊断系统应用规范》明确了系统的性能要求、临床验证流程等，提升了人工智能辅助诊断系统的临床适用性与可靠性。此外，细分领域专用标准还推动了新一代通信技术在特定医疗场景的深度应用，加速了相关技术的产业化进程。

（三）数据安全与隐私保护标准建设

数据安全与隐私保护是新一代通信技术医疗应用的核心关切，相关标准建设备受重视。国家层面出台《数据安全法》《个人信息保护法》等法律法规，为医疗数据安全与隐私保护提供了法律依据；行业层面，国家卫生健康委制定《医疗数据安全指南》《健康医疗大数据安全管理规范》等标准，明确了医疗数据的分类分级、安全防护要求、共享使用规范等；在技术层面，中国通信标准化协会制定《5G 医疗数据传输安全技术要求》，规范了 5G 网络环境下医疗数据传输的加密方式、身份认证、访问控制等技术要求；在管理层面，全国信息安全标准化技术委员会制定《健康医疗数据隐私保护管理规范》，明确了医疗数据采集、存

储、使用、销毁等全流程的隐私保护管理要求。

数据安全与隐私保护标准的建设为新一代通信技术医疗应用筑牢了安全防线。例如,《医疗数据安全指南》将医疗数据分为核心数据、重要数据、一般数据三个级别,针对不同级别数据提出差异化的安全防护要求,确保核心医疗数据的绝对安全;《5G 医疗数据传输安全技术要求》规定了医疗数据在 5G 网络传输过程中必须采用端到端加密技术,防止数据被窃取、篡改。此外,相关标准还推动了医院数据安全管理体系的完善,提升了医院应对数据安全风险的能力。

(四) 标准化建设的协同机制与未来方向

我国新一代通信技术医疗应用的标准化建设形成了多主体协同参与的机制。国家标准化管理委员会、国家卫生健康委、工信部等部门发挥统筹协调作用,明确标准化建设的重点方向与任务分工;行业协会牵头组织标准的制定与推广,协调企业、医院、科研机构等主体参与;龙头企业凭借技术优势,主导或参与关键标准的制定,推动标准与市场需求的对接;科研机构为标准化建设提供技术支撑,开展标准的可行性研究与验证。此外,我国还积极参与国际标准化工作,在 ITU、ISO 等国际组织中推动新一代通信技术医疗应用相关标准的制定,提升我国在国际标准领域的话语权。

未来,新一代通信技术医疗应用的标准化建设将朝着以下方向发展:一是聚焦 6G 医疗应用前沿领域,提前布局 6G+ 医疗健康相关标准的研究与制定,涵盖空天地一体化医疗通信、通感算一体化医疗应用等新场景;二是强化标准的国际化协同,推动我国标准与国际标准的互认,提升我国新一代通信技术医疗应用的国际竞争力;三是完善标准的动态更新机制,根据技术发展与应用需求及时修订标准,确保标准的科学性与时效性;四是加强标准的推广与实施监督,提升标准的落地成效,推动新一代通信技术医疗应用的规范化、高质量发展。

第四节 新一代通信技术在医院信息化管理中的 创新应用面临的挑战与对策

新一代通信技术为医院信息化管理带来了革命性机遇，推动医院管理从传统的经验化、粗放化向精准化、精细化转型，在资源调度、成本管控、服务质量提升、科研教学等领域实现创新应用。然而，在实践过程中，新一代通信技术在医院信息化管理中的创新应用仍面临技术适配不足、数据治理滞后、人才支撑短缺、资金投入压力大、管理机制不健全等多重挑战。针对这些挑战，需要从技术创新、数据治理、人才培养、资金保障、机制改革等多维度制定对策，推动新一代通信技术在医院信息化管理中深度融合、高效应用，提升医院管理水平与服务质量。

一、新一代通信技术在医院信息化管理中的创新应用场景

新一代通信技术凭借其高速率、低时延、广连接、高可靠的特性，在医院信息化管理的多个领域实现创新应用，构建起“智能、高效、协同、安全”的医院信息化管理体系。在资源管理领域，实现医疗设备、药品、床位、医护人员等资源的智能化调度与实时监控；在成本管理领域，通过大数据分析实现运营成本的精准管控与优化配置；在服务管理领域，构建全流程智能化服务体系，提升患者就医体验；在科研教学领域，推动医学科研协同化与医学教育智能化发展；在安全管理领域，实现医疗数据安全与医院运营安全的全方位保障。这些创新应用场景不仅提升了医院管理效率与运营效益，也为患者提供了更加优质、便捷的医疗服务。^①

（一）智能化资源调度与管理

基于 5G、6G 技术与物联网、大数据的融合，医院实现了医疗资源的智能化调度与管理。通过在医疗设备、药品、床位等资源上部署智能传感器与 RFID 标签，借助新一代通信技术的高速传输与广连接特性，实现资源信息的实时采集与动态监控。在设备管理方面，通过智能设备管理平台，实时监控医疗设备的运行状态、维护记录、使用效率等信息，实现设备的预防性维护与高效调度；在药品管理方面，智能药房通过 5G 网络实时接收处方信息，自动完成药品调配与发放，

① 艾蕾. 财务管理信息化在公立医院的应用现状与策略研究 [J]. 中国管理信息化, 2025, 28 (21): 101-103.

同时实时监控药品库存,实现药品的精准采购与库存管理;在床位管理方面,智能床位管理系统实时更新床位使用状态,根据患者病情与诊疗需求智能分配床位,提升床位利用率;在医护人员管理方面,通过人员定位系统实时追踪医护人员位置,在紧急情况下快速调配人力,提升应急响应效率。

（二）精准化成本管控与优化

新一代通信技术推动医院成本管理从传统的事后核算向事前预测、事中控制转型,实现精准化成本管控与优化。通过大数据分析技术,整合医院的人力、物资、能耗、医疗服务等多维度数据,建立成本分析模型,精准识别成本管控的关键点与优化空间。在能耗管理方面,通过智能能耗监测系统实时采集水电油气等能耗数据,结合 AI 算法分析能耗规律,识别能耗浪费点,推送节能建议,降低医院能耗成本;在物资管理方面,通过物资全流程追溯系统,实时监控药品、耗材等物资的采购、入库、使用、报废等环节,减少物资浪费与积压,降低物资成本;在人力成本管理方面,通过人力资源管理系统分析医护人员的工作效率、工作量等数据,优化人员配置,提升人力成本使用效益。此外,新一代通信技术还支持医院开展 DRG/DIP 付费改革相关的成本核算,精准测算不同病种的医疗成本,为医保支付改革提供数据支撑。

（三）全流程智能化服务管理

依托新一代通信技术,医院构建起全流程智能化服务管理体系,覆盖患者就诊前、就诊中、就诊后的全环节,提升患者就医体验。在就诊前,通过智能预约挂号系统、在线问诊平台,患者可实现远程挂号、预约检查、在线咨询等服务,减少现场等待时间;在就诊中,通过智能导诊系统、电子病历系统、移动护理终端等,实现患者信息的实时共享与诊疗流程的智能化衔接,医生可通过移动终端实时查看患者病历、检查结果,开具电子处方,护士可通过移动护理终端完成护理操作与信息录入;在就诊后,通过智慧随访平台、健康管理 APP,医生可实时跟踪患者康复情况,推送个性化康复指导,患者可随时反馈健康问题,实现诊疗与康复的无缝衔接。此外,新一代通信技术还支持医院开展远程医疗服务,将优质医疗资源延伸至基层,提升医疗服务的可及性。

（四）协同化科研与智能化教学管理

新一代通信技术推动医院科研管理向协同化、智能化转型,提升科研创新能力。通过构建多中心科研协同平台,借助 6G 网络的高速传输与全域覆盖特性,

实现不同医院、科研机构之间的科研数据实时共享与协同分析,加快科研项目推进速度;结合 AI 技术,实现科研数据的快速挖掘与分析,发现疾病发病机制、治疗靶点等,提升科研效率。在教学管理方面,新一代通信技术推动医学教育向智能化、沉浸式转型,通过 VR/AR 技术与 6G 网络的融合,构建沉浸式临床技能训练平台,医学生可开展模拟手术、模拟问诊等实践训练;通过远程教学平台,实现优质医学教育资源的跨区域共享,提升医学人才培养质量。此外,医院还可以通过数字化知识管理平台,整合医学文献、临床案例等资源,实现医学知识的高效传播与传承。

(五) 全方位安全管理与风险防控

新一代通信技术为医院安全管理提供了全方位支撑,涵盖医疗数据安全、运营安全、患者安全等多个领域。在医疗数据安全方面,通过 5G/6G 网络的加密传输技术、区块链技术等,实现医疗数据在采集、传输、存储、使用等全流程的安全防护,防止数据泄露、篡改;在运营安全方面,通过智能监控系统、物联网传感器等,实时监控医院消防、安防、设备运行等情况,及时发现安全隐患,发出预警并启动应急响应;在患者安全方面,通过患者身份识别系统、智能用药提醒系统等,防止医疗差错的发生,保障患者诊疗安全。此外,新一代通信技术还支持医院建立应急指挥平台,提升应对突发公共卫生事件、突发灾害事故的应急处置能力。

二、新一代通信技术在医院信息化管理创新应用面临的挑战

尽管新一代通信技术在医院信息化管理中展现出广阔的应用前景,但在实践过程中仍面临诸多挑战,这些挑战涉及技术、数据、人才、资金、管理等多个维度,制约了新一代通信技术的深度融合与高效应用。深入分析这些挑战,对于制定针对性的对策措施、推动医院信息化管理高质量发展具有重要意义。

(一) 技术适配性不足,融合应用深度不够

技术适配性不足是新一代通信技术在医院信息化管理应用中面临的首要挑战。一方面,医院现有信息系统与新一代通信技术的适配性较差,多数医院的 HIS、LIS、PACS 等传统信息系统建设时间较早,技术架构相对陈旧,难以直接对接 5G、6G 网络与智能设备,导致数据交互不畅、系统运行不稳定等问题。例如,部分医院的 PACS 系统无法高效传输 4K/8K 超高清影像数据,影响远程影像诊断

的开展；另一方面，新一代通信技术与医疗设备的融合深度不够，现有医疗设备多采用传统通信接口，与 5G、6G 技术的兼容性不足，难以实现设备的智能化升级与协同工作。此外，6G 技术尚处于研发阶段，相关技术标准与应用场景尚未成熟，在医院信息化管理中的应用面临技术不确定性，增加了医院的应用风险。

同时，技术应用的碎片化问题突出，各医院、各部门往往根据自身需求独立开展新一代通信技术应用项目，缺乏整体规划与协同设计，导致不同系统之间难以互联互通，形成“信息孤岛”。例如，部分医院的智能床位管理系统与智能药房系统分属不同部门建设，采用不同的技术标准，无法实现数据共享，影响资源调度的整体效率。技术适配性不足与应用碎片化问题，制约了新一代通信技术在医院信息化管理中作用的充分发挥。

（二）数据治理能力滞后，数据价值难以释放

数据作为医院信息化管理的核心资产，其治理能力直接影响新一代通信技术的应用成效。当前，医院数据治理能力滞后的问题较为突出，主要表现在以下几个方面：一是数据标准不统一，不同医院、不同系统之间的数据采集规范、编码标准、格式要求存在差异，导致数据难以整合与共享。例如，不同医院的电子病历数据编码不统一，无法实现跨医院数据的有效对比与分析；二是数据质量不高，存在数据缺失、错误、冗余等问题，影响数据的准确性与可靠性。例如，部分医护人员在录入病历数据时存在信息填写不完整、不规范的情况，导致数据无法有效用于科研分析与管理决策；三是数据安全性与隐私保护压力大，随着新一代通信技术的应用，医疗数据的传输与共享范围不断扩大，数据泄露、篡改、滥用的风险增加，给医院数据安全带来巨大挑战；四是数据治理机制不健全，多数医院缺乏专门的数据分析与治理团队，数据治理工作缺乏系统性与持续性，难以实现数据的全流程规范管理。

数据治理能力滞后导致医院海量数据的价值难以释放，无法为医院信息化管理提供有效的数据支撑。例如，由于数据标准不统一与质量不高，大数据分析技术难以有效挖掘数据中的规律与价值，无法为成本管控、服务优化、科研创新等提供精准决策依据；数据安全风险的存在，也制约了医疗数据的共享与应用，影响了跨区域医疗协同与科研合作的开展。

（三）复合型人才短缺，人才支撑体系薄弱

新一代通信技术在医院信息化管理中的创新应用，需要既懂医疗业务、又懂

通信技术与信息技术的复合型人才作为支撑。当前，医院复合型人才短缺的问题较为突出，成为制约技术应用的重要瓶颈。一方面，现有医护人员的信息技术素养有待提升，多数医护人员缺乏对 5G、6G、人工智能、大数据等新一代技术的系统了解，难以熟练使用智能化医疗设备与管理系统，影响了技术应用的效率与效果；另一方面，医院信息化管理团队的医疗业务知识储备不足，多数信息化技术人员缺乏医疗专业背景，无法准确把握医疗业务需求，导致技术应用与业务需求脱节，难以开发出符合医院实际需求的信息化管理解决方案。

此外，复合型人才培养与引进机制不健全，也加剧了人才短缺的问题。高校相关专业设置滞后于行业发展需求，缺乏针对新一代通信技术医疗应用的复合型人才培养方案；医院对复合型人才的引进力度不足，薪资待遇与发展空间难以吸引优秀人才；同时，医院内部缺乏完善的人才培训体系，无法有效提升现有人员的复合型能力。人才支撑体系的薄弱，严重制约了新一代通信技术在医院信息化管理中的创新应用与深度融合。

（四）资金投入压力大，投入产出效益不明显

新一代通信技术在医院信息化管理中的应用需要巨额的资金投入，包括网络基础设施建设、智能设备采购、信息系统升级、人才培养等多个方面。当前，医院面临着巨大的资金投入压力，尤其是基层医院与中小型医院，由于自身运营收入有限，财政支持不足，难以承担新一代通信技术应用项目的高额成本。例如，建设一套完整的 5G+ 智能医院信息化管理系统，涉及基站建设、设备采购、软件研发等多个环节，资金投入往往高达数千万元，这对于多数基层医院而言难以承受。

同时，资金投入的产出效益不明显，也影响了医院的投入积极性。一方面，新一代通信技术在医院信息化管理中的应用成效具有滞后性，短期内难以直接转化为经济效益，导致医院对投入回报的预期不明确；另一方面，缺乏科学的投入产出评估体系，无法准确衡量新一代通信技术应用对医院管理效率提升、成本降低、服务质量改善等方面的贡献，难以为资金投入提供有力的决策依据。资金投入压力大与投入产出效益不明显的问题，制约了新一代通信技术在医院信息化管理中的规模化应用。

（五）管理机制不健全，协同推进力度不足

管理机制不健全是新一代通信技术在医院信息化管理应用中面临的另一重要

挑战。一方面,医院内部缺乏统筹协调机制,新一代通信技术应用项目往往涉及多个部门(如信息科、医务科、护理部、设备科等),但各部门之间缺乏有效的沟通协作,存在各自为政的现象,导致项目推进效率低下,难以形成工作合力。例如,在智能设备采购项目中,设备科负责设备选型,信息科负责系统对接,医务科负责临床应用,由于缺乏统筹协调,可能出现设备与系统不兼容、临床应用需求无法满足等问题;另一方面,医院与外部主体(如通信企业、医疗设备企业、科研机构等)的协同机制不完善,合作模式较为单一,难以实现优势互补、资源共享。例如,医院与通信企业的合作多停留在网络建设层面,在技术研发、应用创新等深度合作方面不足,无法充分发挥企业的技术优势与医院的临床资源优势。

此外,医院信息化管理的绩效考核机制不健全,缺乏针对新一代通信技术应用成效的考核指标,难以调动各部门与医护人员参与技术应用的积极性。管理机制的不健全,导致新一代通信技术在医院信息化管理中的应用缺乏系统性与持续性,难以实现长效发展。

三、推动新一代通信技术在医院信息化管理中创新应用的对策

针对新一代通信技术在医院信息化管理创新应用中面临的挑战,需要从技术创新、数据治理、人才培养、资金保障、机制改革等多维度制定对策,构建“技术适配、数据驱动、人才支撑、资金保障、机制协同”的全方位发展体系,推动新一代通信技术与医院信息化管理深度融合,提升医院管理水平与服务质量。

(一) 强化技术创新与适配,提升融合应用深度

一是加强医院信息系统升级改造,推动传统信息系统与新一代通信技术的适配融合。医院应制定信息系统升级改造规划,逐步淘汰陈旧技术架构,采用云原生、微服务等先进技术,构建灵活、可扩展的医院信息平台,实现与 5G、6G 网络、智能设备的无缝对接。例如,对 HIS、LIS、PACS 等核心系统进行升级,提升系统的数据处理能力与交互能力,支持 4K/8K 超高清影像数据的高效传输与分析;二是推动医疗设备的智能化升级与标准化改造,鼓励医疗设备企业研发具有 5G/6G 通信接口的智能医疗设备,制定医疗设备通信接口的统一标准,提升设备之间的兼容性与协同性。医院在采购医疗设备时,应优先选择符合标准的智能化设备,降低设备与系统的适配成本;三是加强技术应用的整体规划与协同设计,建立医院信息化管理技术应用统筹协调机制,结合医院发展战略与业务需求,

制定新一代通信技术应用整体规划,明确各部门的职责与分工,避免应用碎片化。同时,加强不同系统之间的技术协同,打破“信息孤岛”,实现数据的互联互通与资源的协同调度;四是前瞻布局 6G 技术研发与应用试点,医院可与通信企业、科研机构合作,开展 6G+ 医疗健康应用场景的探索与验证,提前储备相关技术与经验,为 6G 技术的规模化应用奠定基础。

（二）完善数据治理体系，释放数据价值

一是建立健全医疗数据标准体系,推动数据的标准化采集与管理。医院应严格遵循国家与行业相关数据标准,制定医院内部的数据采集规范、编码标准、格式要求,统一电子病历、检查检验结果、医疗设备数据等各类数据的标准,确保数据的一致性与规范性。同时,积极参与行业数据标准的制定与推广,推动跨医院、跨区域数据标准的统一;二是提升数据质量管控水平,建立数据全流程质量管控机制。在数据采集环节,通过智能化数据录入工具(如语音识别、模板化录入等)减少人工录入错误,加强数据录入的审核与校验;在数据存储环节,采用数据清洗、去重、补全等技术,提升数据质量;在数据使用环节,建立数据质量评估机制,定期对数据质量进行检查与评估,及时发现并整改数据质量问题;三是强化数据安全与隐私保护,构建全方位的数据安全保障体系。采用端到端加密、区块链、身份认证、访问控制等先进技术,确保医疗数据在传输、存储、使用等全流程的安全;建立数据安全风险监测与预警机制,实时监测数据异常访问行为,及时处置安全风险;严格遵守相关法律法规,规范医疗数据的共享与使用流程,保障患者隐私权益;四是健全数据治理机制,组建专门的数据分析与治理团队,明确团队的职责与分工,开展系统性的数据治理工作。同时,引入专业的数据治理工具与平台,提升数据治理的效率与效果,充分释放数据价值,为医院管理决策、科研创新、服务优化等提供数据支撑。

（三）加强复合型人才培养与引进，筑牢人才支撑体系

一是优化人才培养模式,培养复合型人才。高校应调整相关专业设置,增设“医学信息工程”“智慧医疗”等复合型专业,构建“医疗+通信+信息”的跨学科人才培养体系,培养既懂医疗业务又懂技术的复合型人才;医院应建立完善的内部培训体系,定期组织医护人员与信息化技术人员开展跨领域培训,提升现有人员的复合型能力。例如,对医护人员开展信息技术培训,提升其智能化设备与系统的使用能力;对信息化技术人员开展医疗业务培训,提升其对医疗需求的

把握能力；二是加大复合型人才引进力度，优化人才激励机制。医院应制定优惠的人才引进政策，通过提高薪资待遇、提供广阔的发展空间等方式，吸引高校毕业生、行业优秀人才等加入；建立科学的绩效考核与激励机制，将技术应用成效、数据治理成果等纳入考核指标，对表现优秀的复合型人才给予表彰与奖励，调动人才的积极性与创造性；三是加强产学研协同育人，医院与高校、企业、科研机构合作，建立实习实训基地，为学生提供实践机会，同时借助外部资源提升医院现有人员的专业能力。例如，与通信企业合作开展技术培训，邀请企业专家为医院人员讲解新一代通信技术的应用与发展趋势；与高校合作开展科研项目，培养科研型复合型人才。

（四）多元化保障资金投入，提升投入产出效益

一是拓宽资金筹集渠道，缓解资金投入压力。医院应积极争取政府财政支持，申报各类智慧医疗、信息化建设专项基金；引入社会资本，通过 PPP 模式、战略合作等方式，与企业合作开展新一代通信技术应用项目，实现风险共担、利益共享；优化医院内部资金配置，合理安排信息化建设资金，提高资金使用效率；二是建立科学的投入产出评估体系，提升资金投入效益。医院应制定新一代通信技术应用项目的投入产出评估指标体系，从管理效率提升、成本降低、服务质量改善、科研创新成果等多个维度评估项目成效；引入专业的评估机构，对项目的投入产出效益进行客观评估，为资金投入决策提供依据；加强项目全流程的资金管理与监督，确保资金专款专用，避免资金浪费；三是推动技术应用的产业化发展，提升长期经济效益。医院可与企业合作，将技术应用过程中形成的创新成果转化为产品或服务，实现产业化发展，形成“应用 - 创新 - 产业化 - 再投入”的良性循环，提升资金投入的长期回报。

（五）深化管理机制改革，强化协同推进力度

一是建立医院内部统筹协调机制，加强各部门之间的沟通协作。成立由医院领导牵头的新一代通信技术应用工作领导小组，统筹协调信息科、医务科、护理部、设备科等相关部门的工作，明确各部门的职责与分工，建立定期沟通会议制度，及时解决项目推进过程中存在的问题，形成工作合力；二是完善医院与外部主体的协同机制，推动深度合作。医院应与通信企业、医疗设备企业、科研机构等建立长期稳定的战略合作关系，构建“产学研用”协同创新体系。例如，与通信企业合作开展技术研发，共同攻克技术适配难题；与医疗设备企业合作开展智

能设备的临床验证与应用推广；与科研机构合作开展科研项目，提升技术应用的科学性与创新性；三是健全绩效考核与激励机制，调动各方积极性。制定针对新一代通信技术应用成效的绩效考核指标，将考核结果与部门评优、个人绩效挂钩；设立技术创新奖励基金，对在技术应用创新中做出突出贡献的部门与个人给予奖励；鼓励医护人员参与技术应用与创新，提出合理化建议，营造全员参与的良好氛围；四是加强医院信息化管理的制度建设，完善相关管理制度与操作规范，为新一代通信技术的应用提供制度保障。例如，制定智能化设备使用管理制度、医疗数据共享管理制度、远程医疗服务管理制度等，规范技术应用流程，确保技术应用的规范化、标准化发展。

参考文献

- [1] 白燕文. “互联网+”背景下公立医院财务信息化管理的现实需求及关键路径 [J]. 中国管理信息化, 2025, 28 (24): 215-217.
- [2] 何菁华. 信息化时代医院工会管理创新与改革实践探索 [J]. 中国信息界, 2025, (11): 198-200.
- [3] 鲁慧. 医院档案信息化管理创新模式 [J]. 数字技术与应用, 2025, 43 (11): 100-102.
- [4] 刘谦,孙婷娇. 基于VPN技术的区域性远程医疗系统的构想 [J]. 医疗设备信息, 2007, (12): 43-45.
- [5] 贾末,计虹,李翠霞,等. 医疗数据共享过程中的信息安全与隐私保护 [J]. 中国数字医学, 2025, 20 (11): 19-24.
- [6] 杨建强. 智慧医院建设背景下会计信息化转型实施策略分析 [J]. 行政事业资产与财务, 2025, (21): 64-66.
- [7] 刘轩. 医院运营效率提升策略与问题研究 [J]. 经济师, 2025, (11): 227-228.
- [8] 艾蕾. 财务管理信息化在公立医院的应用现状与策略研究 [J]. 中国管理信息化, 2025, 28 (21): 101-103.
- [9] 任旭,陈勇,杨秀兰,等. 5G背景下急诊急救体系建设的现状与展望 [J]. 中国急救医学, 2025, 45 (08): 723-726.
- [10] 5G技术全球首次用于灾难医学救援 中国移动与四川省人民医院联合开展5G 应急医疗“高速”救援 [J]. 通信与信息技术, 2019, (04): 14.
- [11] 欧吕平. 物联网技术下医院信息化管理系统的应用研究 [J]. 信息与电脑, 2025, 37 (01): 80-82.
- [12] 赵艳,宋平,朱立峰. 基于物联网的医疗设备信息化平台建设实践 [J]. 中国数字医学, 2024, 19 (03): 68-73.
- [13] 陶皓. 基于物联网技术的智慧医院系统设计 [J]. 数字通信世界, 2023, (04): 83-85.

- [14] 周靖云,蒋清,任健. 云计算在医院信息化管理中的作用及影响 [J]. 现代医院, 2023, 23 (03): 422-424.
- [15] 张杨. 云计算技术在医院后勤信息化建设中的应用研究 [J]. 长江信息通信, 2022, 35 (10): 127-129.
- [16] 陈昊,陈伟,刘利,等. 医疗质量管理云平台的研发与应用 [J]. 中国数字医学, 2016, 11 (11): 80-82+113.
- [17] 张羽翔. 5G环境下远程医疗急救视频传输的计算机网络实时性能分析与优化改进 [J]. 软件, 2025, 46 (10): 141-143.
- [18] 樊怡. 人工智能在公立医院档案管理信息化中的应用探索 [J]. 临床医药实践, 2025, 34 (07): 558-560.
- [19] 王映涛. 人工智能驱动医院信息化建设的现状及管理策略 [J]. 数字技术与应用, 2025, 43 (02): 7-9.
- [20] 刘峰. 区块链技术在医院管理信息化中的应用 [J]. 医疗装备, 2023, 36 (09): 33-36.
- [21] 娄岚清,魏东晓,刘颖. 区块链技术在医院管理中的应用分析 [J]. 现代医院管理, 2022, 20 (04): 78-80.
- [22] 邢昊,赵飞. 区块链技术在医疗医药领域应用困境及改进策略的研究 [J]. 中国数字医学, 2025, 20 (02): 50-56.
- [23] 赵治远,樊利军. 基于边缘计算的医院实时数据采集与处理系统设计 [J]. 信息与电脑, 2025, 37 (14): 87-89.