

团体标准

T/GDWJ XXXX—XXXX

多院区医疗数据中心建设规范

Construction specification for multi-campus medical data center

（征求意见稿）

XXXX—XX—XX 发布

XXXX—XX—XX 实施

广东省卫生经济学会发布

目 录

前 言 III

引 言 IV

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

 3.1 资源池 1

 3.2 弹性 2

 3.3 数据中心 2

 3.4 云计算数据中心 2

4 缩略语 2

5 多院区数据中心基础设施要求 2

 5.1 数据中心架构设计规范 2

 5.2 计算资源建设规范 4

 5.3 存储资源建设规范 5

 5.4 网络建设规范 5

 5.5 灾备中心建设规范 6

 5.6 监控运维中心建设规范 6

 5.7 安全及合规建设规范 7

6 多院区医疗数据中心软件建设要求 8

 6.1 多院区业务协作与资源管理平台 8

 6.1.1 多院区业务协作服务 8

 6.1.2 多院区医疗资源统一管理 9

 6.1.3 多院区统一服务门户 9

 6.2 多院区医疗数据中心 9

 6.2.1 多院区统一标准规范 9

 6.2.2 数据采集 9

 6.2.3 统一调度任务 9

 6.2.4 数据治理 10

 6.2.5 数据管理 10

 6.3 多院区医疗同质化管理 10

 6.3.1 统一患者主索引 10

 6.3.2 患者一体化电子病历 10

 6.3.3 多院区统一标准规范 10

 6.4 多院区综合运营决策分析 11

 6.4.1 经济运行预测 11

 6.4.2 综合绩效评价 11

 6.4.3 持续发展能力 11

附 录 A 12

参 考 文 献..... 13

前 言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文体的某些内容可能涉及专利，本文件的发布机构不承担识别专利的责任。

本文件由广东省卫生经济学会提出并归口。

本文件起草单位：东莞市第六人民医院、广州市妇女儿童医疗中心、东莞市卫生统计信息中心、山东中网云安智能科技有限公司、广东网安科技有限公司、郑州立雪智能科技研究院、中山大学附属口腔医院、中山大学附属第一医院、广东省妇幼保健院、广州医科大学附属第二医院、广东省卫生经济学会、清远市人民医院、连州市人民医院、江门市中心医院、佛山市第一人民医院、连州市医疗总院、东莞市第八人民医院、东莞市凤岗医院、杭州数圭通科技有限公司、杭州美创科技股份有限公司、北京天融信科技有限公司、深圳昂楷科技有限公司、深圳君同云科技有限公司。

本文件主要起草人：熊劲光、曹晓均、陈惠城、陈见、魏书山……。

引 言

健康医疗数据作为重要的基础性战略资源，对医学研究、药物开发、疫情防控及临床医疗等领域的发展至关重要。由于其涉及国家生物安全、基础公共福利、个人隐私、生命健康和基本人权等多方面问题，应用中需要特别关注数字科技与医学伦理等创新中的多重未知风险。因此，健康医疗数据流通、共享和应用的合规与风险治理，需要从国家数字化战略、健康医疗事业发展规划、健康医疗事业专业规范以及个人基本人权保障等多个方面实现全流程合规开展。依据《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》以及行业领域的法律法规，参照专业领域规章、信息安全规范标准以及技术标准，制定本标准。

本标准旨在促进健康医疗数据高效应用、合规流通和共享，提升健康医疗数据合规流通共享对健康卫生事业和个人生命健康权益的优化效益，并为健康医疗数据合规流通共享和创新应用中的国家安全、社会公共利益与个人隐私及相关信息权益提供更高层次的保障。本标准主要为健康医疗行业数据流通与共享提供合规实践指引。

如有未尽事项，或相关事项因立法、法律修改等事由在法律法规等规范文件中另有规定的，应依法遵循相关法律法规规定。

多院区医疗数据中心建设规范

1 范围

本标准规定了整体架构、资源池、灾备、运行维护、安全及数据中心统一管理平台软件等基本要求。

本标准适用于设计和建设多院区数据中心基础架构,也可作为制定多院区数据中心相关技术标准、测评标准的依据。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 34982-2017 云计算数据中心基本要求

GB/T 31167-2023 信息安全技术云计算服务安全指南

GB/T 32400-2015 信息技术云计算概览与词汇

GB50174-2017 数据中心设计规范

GB/T 22239-2019信息安全技术网络安全等级保护基本要求

WS/T 303—2023 卫生健康信息数据源标准化规则

WS/T 304—2023 卫生信息数据模式描述指南

WS/T 305—2023 卫生健康信息数据集元数据标准

WS/T 306—2023 卫生健康信息数据集分类与编码规则

WS/T 500-2016(所有部分) 电子病历共享文档规范

WS/T 445-2014(所有部分) 电子病历基本数据集

WS/T 598-2018(所有部分) 卫生统计指标

WS 599-2018(所有部分) 医疗机构人财物运营管理基本数据集

T/GZBC 36-2020 广东省健康医疗数据脱敏技术规范

T/GZBC 37-2020 医疗机构数据治理规范

3 术语和定义

GB/T32400-2015界定的以及下列术语和定义适用于本文件。

3.1 资源池

云计算数据中心提供的物理或虚拟资源的聚合。

3.2 弹性

云计算数据中心的场地、设施和资源池按需分配、回收和调整的能力。

3.3 数据中心

由计算机场地、配套基础设施、信息系统硬件(物理和虚拟资源)、信息系统软件、信息资源(数据)和人员以及相应的规章制度组成的组织。

3.4 云计算数据中心

支撑云计算服务的数据中心。

4 缩略语

下列缩略语适用于本文件：

HIS：医院信息系统（Hospital Information System）

5G：第五代移动通信技术（5th Generation Mobile Communication Technology）

IaaS：基础架构层（Infrastructure as a Service）

PaaS：平台服务层（Platform as a Service）

SaaS：应用服务层（Software as a Service）

CPU：中央处理器（Central Processing Unit）

API：应用程序编程接口（Application Programming Interface）

IT：信息技术（Information Technology）

VPN：虚拟专用网络（Virtual Private Network）

DDos：分布式拒绝服务（Distributed Denial of Service）

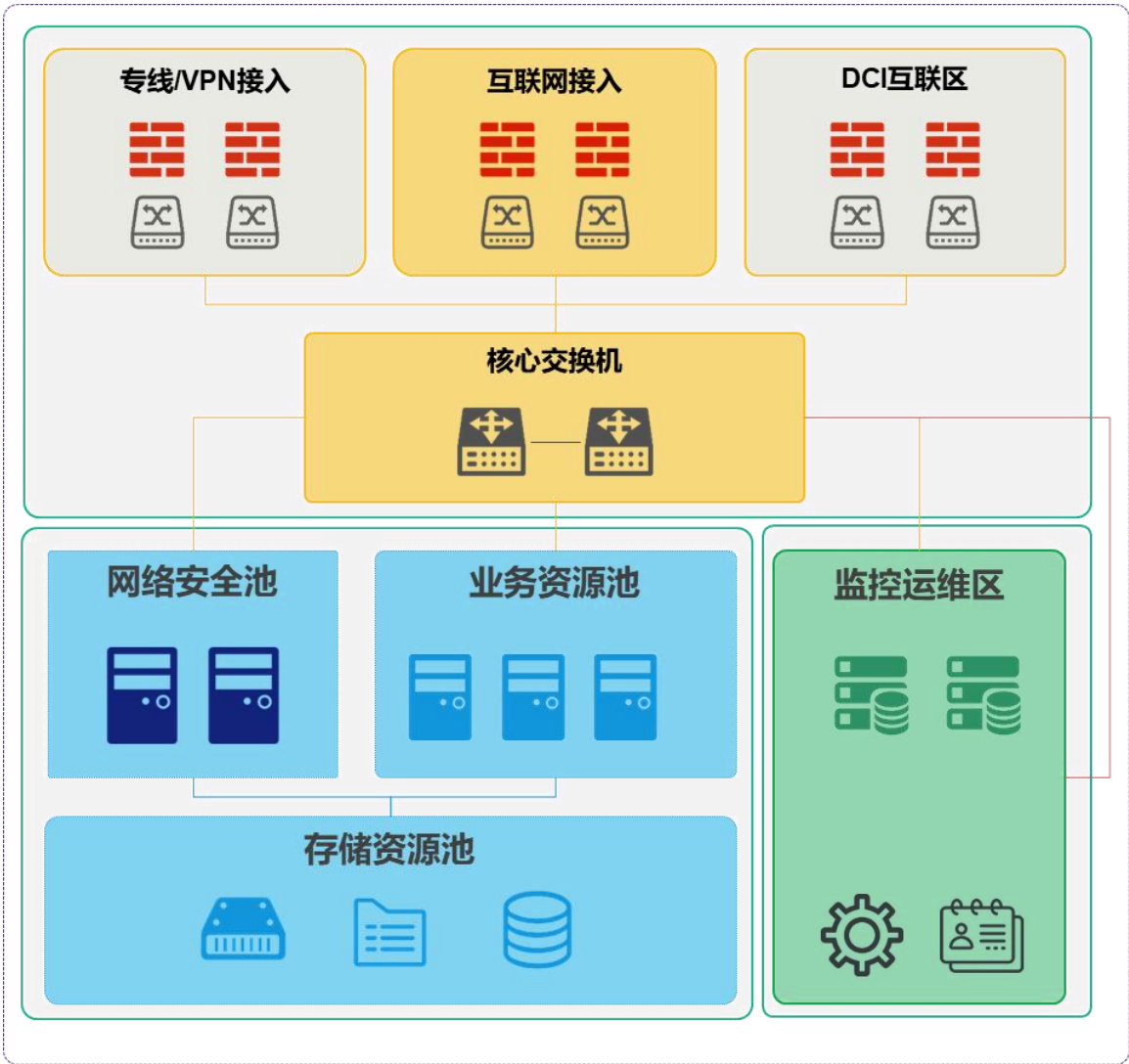
DCI：数据中心互联（Data Center Interconnect）

5 多院区数据中心基础设施要求

5.1 数据中心架构设计规范



多院区互联两地三中心整体架构规范示意图



多院区医疗数据中心架构示意图

- 多院区医疗数据中心（非云场景）架构设计规范：
 - a) 在多个地理位置上建立的数据中心，由医院统一管理，用于支持其业务运营和信息

技术需求；

- b) 数据中心分布在不同的地理位置，可以是同一城市的不同区域，也可以是不同的城市或地区；
- c) 数据中心可以是医院的自建机房，也可以是第三方数据中心机房；
- d) 在主/备数据中心建设中应将计算、存储、网络、安全、管理等不同资源分区建设；
- e) 针对数据中心每个区域资源应采用合理的监控运维平台实现对基础架构设备的统一运维管理。

- 云计算/虚拟化架构设计规范：

- a) 建设一套逻辑上统一的云资源管理平台，在资源层面实现无缝管理，在业务层面实现业务服务统筹运营；
- b) 云平台引入自动化工具和脚本，简化虚拟机和容器的部署、配置和管理过程，提高效率和一致性；
- c) 实施全面的性能监控和优化策略，确保虚拟化环境中的资源利用率和性能达到最佳状态；
- d) 具备虚拟化环境的安全隔离能力，确保不同用户之间的资源和数据隔离，防止数据泄露和未经授权的访问。

5.2 计算资源建设规范

- 多院区医疗数据中心（非云场景）计算资源建设规范：

- a) 支撑计算资源运行的物理主机应采用多核心处理器；
- b) 物理主机的系统软件应可适应多核心的操作系统、编程环境和运行时环境支撑；
- c) 支持提供可动态调整的 CPU、内存、存储、输入输出设备等资源以满足用户业务需求；
- d) 支持在物理机资源或虚拟机资源上的部署和管理，并至少支持分布式、集群或负载均衡其中一种能力。

- 云计算/虚拟化计算资源建设规范：

- a) 至少支持两种虚拟化产品部署；
- b) 支持划分不同层次的计算资源以满足不同规格的计算资源需求；
- c) 应配置虚拟机管理器以实现单物理主机上多虚拟主机管理与配置，提供弹性扩展能力；
- d) 计算资源池管理平台应具有执行过程的高可靠性和随云计算数据中心节点规模的

增长而具有的高扩展性；

- e) 支持主流容器化技术，如 Docker 和 Kubernetes，以提高应用的部署和管理效率。

5.3 存储资源建设规范

- 多院区医疗数据中心（非云场景）存储资源建设规范：
 - a) 支持数据的分层存储及数据的生命周期管理；
 - b) 支持数据在传输和存储过程中的加密，确保数据安全；
 - c) 支持数据压缩和去重技术，减少存储空间以提高存储效率；
 - d) 兼容多种的存储方式，满足计算、网络等资源池的访问要求；
 - e) 支持多种数据类型的数据存取；
 - f) 具备冗余的数据存储能力，并能够实现存储资源的动态调整、数据高可用性、数据迁移、自动精简配置；
 - g) 支持多种存储系统的统一管理；
 - h) 支持存储多路径技术；
 - i) 具备完整性保障机制；
 - j) 具备本地数据备份能力，宜提供异地数据灾备能力；
 - k) 具备存储性能优化功能，如智能缓存、负载均衡等，以提高存储访问速度和效率。
- 云计算/虚拟化存储资源建设规范：
 - a) 存储资源池包括基于对象的云存储和基于键值的云存储；
 - b) 支持自动化存储管理，包括自动化配置、监控和故障处理；
 - c) 支持多云环境的兼容性，能够在不同云平台之间无缝迁移和管理存储资源；
 - d) 云管平台能够通过对多台异构物理存储设备的识别和管理实现资源池化。

5.4 网络建设规范

- 多院区医疗数据中心（非云场景）网络资源建设规范：
 - a) 支持多样化业务，满足流量特性和行为要求；
 - b) 实现网络资源动态调整，实现不同网络协议和网络带宽的选择；
 - c) 支持业务在不同网络环境之间平滑迁移；
 - d) 网络资源具备冗余性和高可用性；
 - e) 支持主流的网络协议，实现与主流云计算服务平台及计算资源池的对接；
 - f) 支持网络优先级管理；

g) 部署网络自动化运维工具，实现网络配置和管理的自动化。

- 云计算/虚拟化网络资源建设规范：

- a) 支持网络虚拟化技术，提升网络管理的灵活性和可扩展性；
- b) 支持多用户和多业务对网络协议和带宽要求；
- c) 实现不同用户或不同业务之间的虚拟网络资源隔离。

5.5 灾备中心建设规范

- 多院区医疗数据中心（非云场景）灾备中心建设规范：

- a) 支持关键数据库系统、应用服务器的实时复制及高可用，当数据出现损坏丢失等问题时可从灾备系统中任意点恢复数据至本地应用，从而实现业务不会因为数据丢失、损坏而导致对外中断服务；
- b) 通过在两个地理位置上设置三个数据中心来实现数据的备份和恢复，这种策略包括：生产中心、同城容灾中心、异地容灾中心；
- c) 使用可靠的备份解决方案定期进行数据备份，包括但不限于磁盘、磁带、云存储等。实施多点备份，包括本地和异地备份，以防止区域性的灾难影响；
- d) 定期进行灾备计划的测试和演练，验证灾备方案的有效性。基于测试结果进行必要的调整和优化，定期更新灾备计划。

- 云计算/虚拟化灾备中心建设规范：

- a) 支持多云环境的兼容性，能够在不同云平台之间无缝迁移和管理灾备资源；
- b) 采用多点备份策略，包括本地和异地备份，使用磁盘、磁带、云存储等多种备份介质，确保数据安全。

5.6 监控运维中心建设规范

- 多院区医疗数据中心（非云场景）监控运维中心建设规范：

- a) 建设统一的监控平台，整合各类监控工具和数据源，实现对计算、存储、网络等资源的统一监控和管理；
- b) 引入自动化运维工具，实现自动化监控、告警、故障处理和资源调度，减少人工干预，提高运维效率；
- c) 利用大数据和人工智能技术，对监控数据进行智能分析，预测潜在故障，优化资源配置。

- 云计算/虚拟化监控运维中心建设规范：
 - a) 云管理平台管理应用运行的操作系统环境及资源, 支持物理机、虚拟机及云环境的基础设施层, 并支持运行在 IaaS 或物理机之上架构的应用;
 - b) 云管理平台能够提供面向云用户和云监管人员的统一接入门户, 通过界面集成、数据集成及功能集成等技术将各个子系统中的功能和信息有效组织起来, 提供统一的信息服务功能入口, 提供用户、授权、认证管理;
 - c) 云管理平台运维控制台提供从 IT 资产配置管理到云产品服务再到应用的立体化多层次运维管理能力, 包含从物理设备到云资源的配置运维服务能力和 IT 资产配置管理能力, 实现数据互通, 与平台的监控告警等能力联动, 实现资源纳管、监控、自动化作业一体化;
 - d) 用户控制台面向用户, 前端资源使用用户提供可视化管理资源能力, 并提供资源分权分域操作的权限管理能力;

5.7 安全及合规建设规范

- 多院区医疗数据中心安全及合规（非云场景）建设规范：
 - a) 根据等级保护 3 级防护要求进行通信网络保护, 通信网络应当有网络安全监控、网络审计、网络备份/冗余与故障恢复、网络应急处理、网络数据传输安全性保护以及可信网络连接设备。综合采用网络安全审计、设备冗余、VPN 网关等技术来实现通信网络保护要求;
 - b) 数据中心网络中心区域边界应当按照 3 级强度进行保护, 通过选择防火墙、入侵防御、入侵检测、防病毒网关等技术满足三级系统的区域边界访问控制、区域边界包过滤、区域边界安全审计、区域边界完整性保护等安全要求;
 - c) 构建一个安全计算环境应当考虑依照保护等级的不同, 分别进行加强用户身份鉴别、自主访问控制、标记和强制访问控制、系统安全审计、用户数据完整性保护、用户数据保密性保护、系统安全监测等措施, 在技术上通过操作系统加固、安全审计、主机防病毒、终端安全管理等措施来实现整体的保护;
 - d) 数据中心接入互联网, 需要在接入位置进行安全隔离, 并且在网络内部各安全域间进行逻辑隔离。
- 云计算/虚拟化安全及合规建设规范：
 - a) 提供安全服务能力（安全 SaaS 云），包括在安全管理、安全防护、安全监测等方面。根据自身业务特点自主设置安全防护策略, 对进出网络的数据和流量进行审计与分析, 发现安全威胁, 对云平台划分的虚拟资源进行集中管理与集中审计。

- b) 安全云管理平台是用户安全管理的核心，定义各类标准安全服务，可同时纳管多种安全产品，如态势感知、日志审计、防火墙、入侵检测、防病毒、VPN、负载均衡、WAF、数据库审计、堡垒机、漏扫，抗 DDos 等。

6 多院区医疗数据中心软件建设要求

通过多院区医疗数据中心建设，实现各院区间数据互联互通、业务共享协同、管理统一高效，加强院区间的分工协作,推进同质化医疗。整个功能框架包括多院区业务协作与资源管理平台、多院区医疗数据中心、多院区医疗同质化管理、多院区综合运营决策分析四部分。见下图所示：

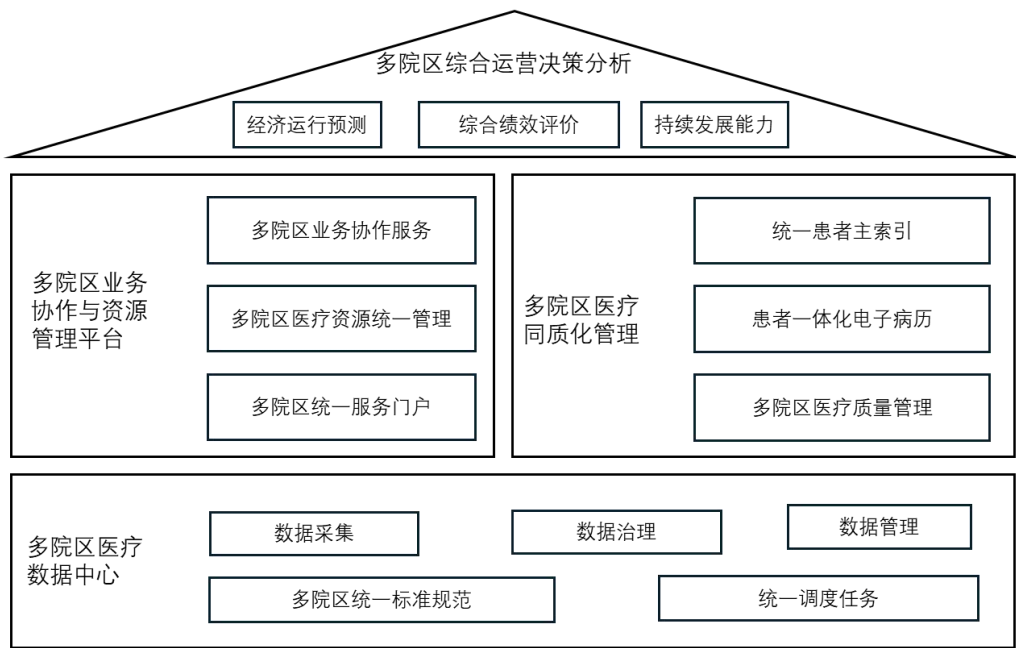


图 多院区数据中心软件功能框架（修改）

6.1 多院区业务协作与资源管理平台

6.1.1 多院区业务协作服务

多院区管理结构复杂，创建多院区业务协作服务可根据医院各院区信息化建设现状以及实际需求进行设计，但系统至少满足：业务协作流程规范高效、院区间业务数据交互顺畅、角色定位和权限明晰、通过数据校验保障协作全环节的数据质量、数据多院区协同共享。

6.1.2 多院区医疗资源统一管理

多院区管理结构复杂，创建多院区业务协作服务可根据医院各院区信息化建设现状以及实际需求进行设计，但系统至少满足：业务协作流程规范高效、院区间业务数据交互顺畅、角色定位和权限明晰、通过数据校验保障协作全环节的数据质量、数据多院区协同共享。

实现对各个院区人财物等各项医疗资源进行统一管理：

- a) 人力资源统一管理：创建统一的人力资源数据库，为院区所有医师制订档案，覆盖医师的基本信息、岗位任职、处方权资质、技术资质、规培记录等，同时对所有院区的医师进行统一人事考勤管理，加强不同院区间人员考勤的有效衔接和全过程管理；
- b) 财务统一管理：要求根据最新政策内容，对所有院区的预算、执行、核算、决算、预算绩效进行统一化、全过程管理，确保各院区在财务信息的录入、处理、审核和报告等方面的一致性和准确性；
- c) 物资统一管理：在多院区财务统一管理基础上，实现对所有院区物资的统一购置、入库、领用、盘点、报废等的全生命周期管理。

6.1.3 多院区统一服务门户

面向各院区提供一站式门户服务，使工作人员通过统一门户，即可享用权限内的各项应用服务。

6.2 多院区医疗数据中心

6.2.1 多院区统一标准规范

多院区医疗数据中心的数据遵循统一的数据标准规范。采用 WS/T 303—2023、WS/T 304—2023、WS/T305—2023、WS/T 306—2023 的标准数据元和数据集。

对于多院区医疗数据中心的主要业务和相关数据，符合“国家卫生健康委办公厅关于印发全国医院数据上报管理方案（试行）的通知（附件）”、“国家卫生健康委办公厅关于印发国家三级公立医院绩效考核操作手册（2024版）的通知（附件）”、“广东省卫生健康委关于印发《三级医院评审标准（2022年版）广东省综合和专科医院实施细则》的通知（附件）”及 WS/T 500（所有部分）里的有关规定。

6.2.2 数据采集

采集各个院区的医疗数据，以制订的多院区统一标准规范为依据，对采集的数据进行预处理，做到标准统一、术语规范、数据准确。

6.2.3 统一调度任务

对数据采集的各项工作流进行统一管理和维护，支持管理员对所有工作流进行统一编排、设置工作流状态；出现问题时能够及时发出告警通知，提醒管理员进行处理，能够支持管理员迅速追根溯源，处理问题。

6.2.4 数据治理

构建数据治理流程，进行数据治理过程的监控和评价：

- a) 构建和运行：构建数据治理实施的机制和路径，以医疗业务规则等为指导构建数据治理规则库，确保数据治理实施的有序进行；
- b) 监控与评价：构建数据治理绩效评价体系，制订评价规则和流程，监控数据中心数据治理的过程，评估数据治理各阶段成效，生成数据治理分析报告；
- c) 改进和优化：根据数据治理监控与评价结果，持续改进数据治理方案，优化数据治理实施策略、方法、流程和规则，促进数据治理方案的不断完善，保障数据质量。

6.2.5 数据管理

对多院区数据中心的所有数据进行统一管理，支撑各项数据应用服务：

- d) 建立数据分层分类管理体系；
- e) 建立完整的数据字典、数据模型、数据架构及其管理体系；
- f) 建立数据管理机制，明确数据管理过程及角色、职责；
- g) 建立数据创建、维护、整合、存储、分发、查询、报告和分析机制；

6.3 多院区医疗同质化管理

6.3.1 统一患者主索引

制定一套完整的标准化算法及数据匹配算法，支持新建或合并多院区患者主索引，针对每个患者生成整个医院多个院区唯一的患者主索引。

6.3.2 患者一体化电子病历

遵循 WS/T 500-2016 共享文档电子病历共享文档规范和多院区统一标准规范，面向每个患者生成整个医院多个院区唯一的患者一体化电子病历，覆盖患者历年历次在多个院区的所有诊疗信息，包括医嘱处方、检验、检查、手术麻醉、会诊、死亡等详细信息。

6.3.3 多院区统一标准规范

落实《医疗质量管理办法》，实现多院区医疗质量管理，推进医院高质量发展：

- a) 建立医疗质量管理知识库，内置统一医疗质量管理制度、临床诊疗规范和标准；
- b) 建立院科两级安全管理体系，开展医院各院区医疗质量安全日常管理工作活动；
- c) 建立医疗质量监管机制，形成对医院各院区人、技、料、法、环的全面质量监管；

- d) 建立医疗质量评价管理，设置考核方案、进行考核评分并生成考核结果，结合PDCA持续改进管理工具，对院区、科室和医师的质量评价进行统一管理。

6.4 多院区综合运营决策分析

以整个医院所有院区为整体，统筹监管，满足医院管理者对医院整体运营宏观决策需要，提供相关的数据支撑及决策依据。

6.4.1 经济运行预测

基于医院现有运营数据，支持经济运行预测模型构建及预测分析：

- a) 支持综合经济预测，通过构建资源要素与经济运行产出的预测模型；
- b) 支持调整相关资源要素投入或流程优化改进，为医院管理者提供决策分析数据；
- c) 支持专项经济预测，对绩效投入、新技术引入、新基建投入等某项变化而引起的经济运行变化的预测，为医院管理者提供经济数据分析。

6.4.2 综合绩效评价

对全院开展综合绩效评价，通过构建资源投入与产出逻辑分析模型、医疗资源服务能力模型等，对医院整体运营效率进行绩效分析。

6.4.3 持续发展能力

开展全院持续发展能力的量化分析，通过对学科建设与能力、人员结构与人才培养、科研能力等各方面，对医院的可持续发展能力进行分析。

附 录 A

（资料性）

跨网数据交换安全技术要求示例

参 考 文 献

- [1] GB/T 37964—2019 信息安全技术 个人信息去标识化指南
 - [2] GB/T 35273—2020 信息安全技术 个人信息安全规范
 - [3] GB/T 39335—2020 信息安全技术 个人信息安全影响评估指南
 - [4] GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型
 - [5] GB/T 39725—2020 信息安全技术 健康医疗数据安全指南
 - [6] GW 0205—2014 国家电子政务外网跨网数据安全交换技术要求与实施指南
 - [7] MH/T 0073—2020 中 华 人 民 共 和 国 民 用 航 空 行 业 标 准
 - [8] Q/CR 855-2021 中国国家铁路集团有限公司企业标准
 - [9] FYB/T 53001-2017 安全隔离与信息交换平台建设要求
-