ICS 35.240.99
CCS L60

T/GYJS

团　　体　　标　　准

T/GYJS 012—2025

区域医疗混合云异地多活数据中心技术规范

Technical Specification for Regional Medical Hybrid Cloud Multi-Site Active Data Centers

2026－01－28 发布　　2026－02－01 实施

广东省云计算应用协会　　发 布

目　　次

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。

本文件由中国医学科学院阜外医院深圳医院、深圳市第四人民医院提出。

本文件由广东省云计算应用协会归口。

本文件起草单位：中国医学科学院阜外医院深圳医院、深圳市第四人民医院、广州医科大学附属妇女儿童医疗中心、广东慧云科技股份有限公司、广州市番禺区卫生健康局、北京志凌海纳科技股份有限公司、广州市弘宇科技有限公司、深圳市南山区医疗集团总部、深圳大学附属华南医院、深圳市第三人民医院、深圳市南山区人民医院、深圳市龙岗区人民医院、深圳市坪山区人民医院、深圳市龙华区妇幼保健院、深圳市中医院、深圳市龙岗区第五医院、广州医科大学附属第二医院、广州医科大学附属第五医院、广州医科大学附属番禺中心医院、广州市第一人民医院、广州开发区医院、广州市番禺区中医院、广州市番禺健康管理中心（广州市番禺区康复医院）、番禺区医疗卫生集团、中山大学附属第三医院、中山大学孙逸仙纪念医院、中山大学肿瘤防治中心、南方医科大学珠江医院、广东省第一荣军优抚医院、中山大学附属口腔医院、南方医科大学附属第三医院、中山市人民医院、暨南大学附属顺德医院、佛山市顺德区中西医结合医院、广东医科大学顺德妇女儿童医院、顺德区第三人民医院、佛山市顺德区第四人民医院（佛山市顺德区伍仲珮纪念医院）、中山大学附属第三医院肇庆医院、粤北人民医院、连州市医疗总院、广州市南沙区东涌镇东涌社区卫生服务中心、广州市南沙区大岗镇灵山社区卫生服务中心、广州市南沙区东涌镇鱼窝头社区卫生服务中心、广州市南沙区珠江街道社区卫生服务中心、中山大学国家超级计算广州中心、国家超级计算长沙中心、中国电信股份有限公司广州分公司、中国移动通信集团广东有限公司广州分公司、中国联合网络通信有限公司广州分公司、广东省通信产业服务有限公司、深圳市棒可可科技有限公司、广东飞和信息科技有限公司、暨南大学、西安电子科技大学、中南大学、湖南大学、广东药科大学、广东工业大学、广东技术师范大学、西安邮电大学、西华大学、上海电力大学。

本文件主要起草人：刘化龙、查正清、宗慧、欧阳杰、苏榕彬、王健英、杨川川 、唐雄伟、徐飞、王逸欣、李鹏、吴庆军、李贵华、练剑锋、任英华、谭建皓、何颖新、刘斌、陈汉威、林志辉、力竟成、廖颖研、张泽彬、李世君、陈玉兵、吴庆斌、郑华国、林汉辉、龙运艺、黄幸青、张晓东、吴向群、陈智斌、李国练、邹志武、张家庆、王永祥、蔡勇、桑宝珍、邓意恒、廖茂成、任忠敏、王文辉、高峰、李博孜、周日文、罗雪琼、郑毅强、谢显荣、郭华星、苏悦洪、梁润锦、鲁俊杰、邓亚萍、张雀屏、欧阳少谦、邓悦森、陈景良、陈桂能、陈志福、雷淦淇、张浩然、岳浩、蔡永铭、李斯钰、杨进、宋京、黄礼高、刘可儿、黄玉辉、王铿、赵伍杰、郑东生、曾安、雷前、任方、杨腾飞、潘丹、张嘉鹏、刘志全、林舒源、苗银宾、王亮亮、杨宝瑶、唐卓、周望、刘玉娟、庾燕莉。

引　言

数字时代，政企业务上云已成为大势所趋。虽然上云可为政企用户带来业务应用部署调度更加灵活、资源利用率更高的优点，但因云平台建设处于不同的阶段，且运转过程中包含大量的、不同类型的业务系统和应用场景，在整体云平台的建设中往往会产生如公有云、私有云、信创云、非信创云等不同架构、不同模式、不同厂商的云平台。多云并存模式是应对 IT 多元化的必然选择，然而随着其广泛应用，集中、统一的多云纳管、混合云运维愈发凸显其重要性。因此，制定《区域医疗混合云异地多活数据中心技术规范》对于推动区域医疗信息化的高质量发展具有重要意义。

区域医疗混合云异地多活数据中心技术规范

1 范围

本文件规定了区域医疗混合云环境下异地多活数据中心的技术架构、关键技术和数据管理，适用于智慧医疗系统建设中的容灾备份、业务连续性保障及数据互操作场景。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 20988-2025 网络安全技术 信息系统灾难恢复规范
GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求
GB/T 24364-2023 信息安全技术 信息安全风险管理实施指南
GB/T 25070-2019 信息安全技术 网络安全等级保护安全设计技术要求
GB/T 31168-2023 信息安全技术 云计算服务安全能力要求
GB/T 37964-2019 信息安全技术 个人信息去标识化指南
GB/T 39725-2020 信息安全技术 健康医疗数据安全指南
GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求
GB 50174-2017 数据中心设计规范
WS/T 787-2021 国家卫生信息资源分类与编码管理规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

区域医疗混合云 Regional Healthcare Hybrid Cloud
指结合本地数据中心和公有云资源，为区域医疗业务提供弹性计算、存储、网络及服务云计算架构。

3.2

异地多活数据中心 Multi-Site Active Data Center
指分布在多个地理位置的独立数据中心，通过协同调度实现业务流量动态分配和数据实时同步，确保高可用性和容灾能力。

3.3

混合云架构 Hybrid Cloud Architecture
通过统一管理平台整合私有云与公有云资源，实现数据互通、负载均衡和安全策略协同的技术框架。

3.4

云原生技术 Cloud-Native Technology
基于容器化、微服务和DevOps的架构方法，支持医疗应用快速部署、弹性伸缩和自动化运维。

3.5

全局调度层 Global Scheduling Layer
通过智能路由和负载均衡算法，动态分配用户请求至最优数据中心系统组件，支持跨机房无感知切换。

3.6

分布式事务框架 Distributed Transaction Framework

保障跨数据中心操作原子性（ACID）的技术方案，包含事务补偿、回滚及冲突解决机制。

3.7

医疗数据交换平台 Healthcare Data Exchange Platform

连接不同医疗机构、系统及用户，实现医疗健康数据安全、标准化交换与共享的核心信息基础设施。其核心目标是打破“信息孤岛”，让数据在不同系统间安全、顺畅地流动，从而提升医疗服务质量与效率。

3.8

个人健康医疗数据 personal health data

单独或与其他信息结合后能够识别特定自然人或者反映特定自然人生理或心理健康相关电子数据。

3.9

健康医疗数据 health data

包含个人健康医疗数据以及由个人健康医疗数据加工处理之后形成的健康医疗相关电子数据。

4 参考模型

本模型为区域医疗混合云环境下异地多活数据中心的建设提供统一的架构指导，确保高可用、高安全、低延迟、数据一致性及业务连续性。模型从数据层、业务层、安全层、运维层和基础实施层五方面做规范。

4.1 模型设计原则

a) 合规性保障：数据在存储、传输与共享全生命周期中，应符合国家网络安全等级保护 2.0 三级及以上要求、《中华人民共和国个人信息保护法》及相关医疗数据安全规范；
b) 业务连续性：异地多活架构需支持核心业务在故障或切换场景下自动切换；
c) 资源性调度：结合混合云特性，公有云承载非敏感弹性业务，私有云承载核心敏感业务；
d) 区域协同兼容：支持区域内不同级别医疗机构数据互通，兼容现有医疗系统，避免数据孤岛。

4.2 总体架构

基于全面覆盖业务、数据、安全、运维与基础设施层的区域医疗混合云异地多活数据中心模型架构应符合图1，该架构系统性地支撑了医院核心业务与创新应用的协同发展。

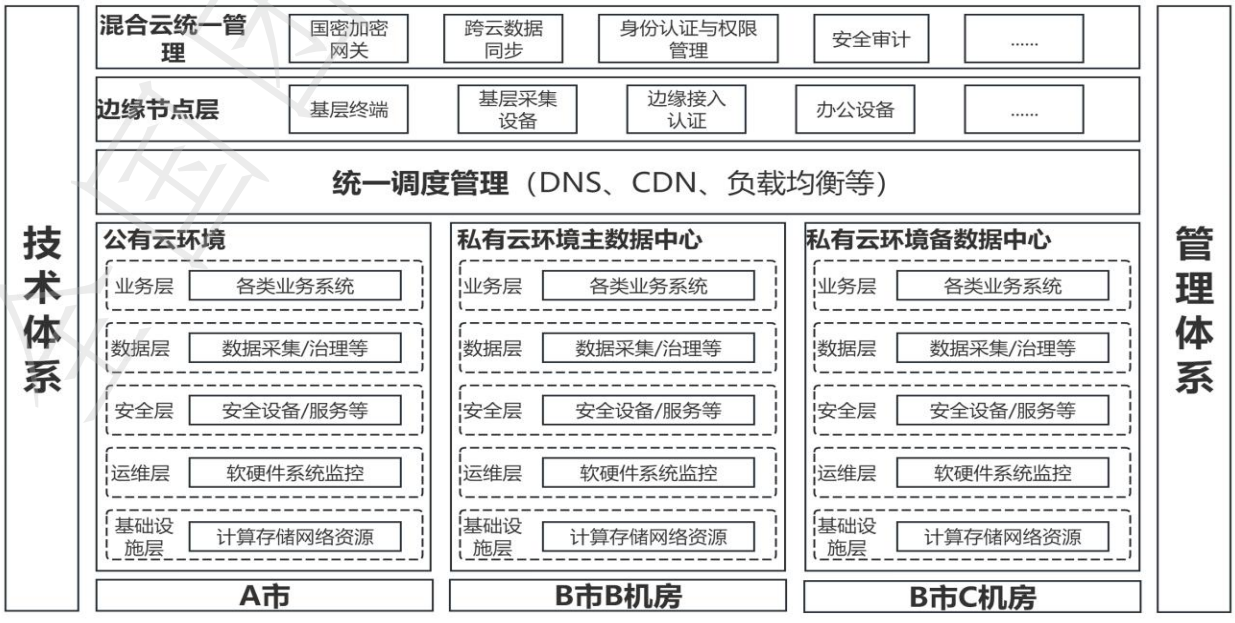

图1　区域医疗混合云异地多活数据中心模型架构图

区域医疗混合云异地多活架构采用 “私有云 + 公有云 + 边缘节点” 三层架构，实现资源分层管控与弹性扩展。核心要求如下：

a) 私有云层（主/备数据中心，如地理位置分别为 B 市的 B 和 C 两个不同物理机房）部署 EMR、HIS、LIS 等高敏感核心系统，采用虚拟化+分布式存储，依托开放式平台实现资源池化与高可用；
b) 公有云层（合规医疗公有云，如地理位置在 A 市）承载非敏感/高弹性/计算密集型业务，基于容器化、对象存储、Serverless 架构，支持按需伸缩与成本优化；
c) 边缘节点层（基层医疗机构）支撑低延迟本地化场景，部署轻量化网关+本地缓存，实现断网续传、就近计算；
d) 主/灾备中心双 Region 部署且网络三层互通，中间件支持双 Region 实例部署，兼容数据同步/不同步模式，数据库、对象存储跨 Region 容灾并支持故障手工切换；
e) 主/灾备节点地理距离≥50 公里，全量部署混合云实现双活互备，通过 DNS/专用设备实现全局负载均衡，采用 “专线 +VPN 备份” 链路保障核心数据分钟级同步，设第三方仲裁节点，网络中断时投票判定活跃节点，故障恢复后校验解锁。

5　通则

5.1　混合云架构设计

5.1.1　核心业务本地化

5.1.1.1　关键医疗业务数据部署在本地数据中心

a) 业务数据范畴：涵盖 HIS 全量核心数据，包括患者身份标识、诊疗记录、药品耗材管理、医疗收费、医护人员执业信息等；
b) 本地数据中心选址与配置：选址紧邻核心医疗机构以降低传输延迟，并配置企业级服务器及大容量高读写存储阵列等硬件设施；
c) 采用云计算资源池建设模式：整合现有资源，动态扩展配置，实现服务资源集中管理。

5.1.1.2　确保数据安全性和高可用性

a) 高可用存储系统核心特性
   1) 数据冗余与故障恢复：应支持 2 副本、3 副本及纠删码等数据冗余策略，在硬盘或节点故障后可自动利用可用空间恢复数据分布，并支持通过故障域划分避免单一故障影响；
   2) 运维智能与安全保障：应支持自动探测并隔离异常磁盘，且具备智能调整数据恢复与迁移速率的能力，确保不影响业务 I/O；
   3) 硬件虚拟化与加密支持：应支持对虚拟卷进行静态加密保护，支持通过 SR-IOV 直通及 MDEV 直通等方式挂载加密控制器设备。
b) 数据安全防护体系
   1) 网络安全与防护：应实施静态数据加密与动态传输加密，并采用防火墙体系进行网络隔离；部署入侵检测与防御系统以实时监测和抵御网络攻击；
   2) 数据备份与可用性：应建立数据备份机制，结合本地与异地策略确保数据可恢复性；同时制定并执行容灾恢复方案，保障业务连续性；
   3) 数据安全与合规管理：应部署日志审计与数据脱敏系统，建立覆盖敏感数据全生命周期的安全管控与脱敏机制，满足数据留存与使用合规要求。
c) 高可用性保障体系
   1) 架构冗余设计：数据库主从集群（30s 内自动切换）、存储阵列双控制器、网络冗余拓扑；
   2) 设备巡检与维护：每日远程检查、每周现场检查、每月深度维护，闭环处理潜在故障；
   3) 应急预案制定：明确应急流程与责任分工，定期演练。

5.1.2　非核心业务云扩展

为提升资源利用率并降低本地基础设施运行负担，非核心业务（互联网医疗、科研计算、健康管理等）应在满足安全与合规要求的前提下，采用公有云服务实现弹性扩展。具体应满足以下要求：

a) 业务适配性：选择在公有云部署的系统应具备资源需求伸缩性较大、业务时延敏感度较低（时延在 100ms 内不影响使用体验）的特征。

b) 平台与技术要求

1）公立云平台须具备国家或行业认可的安全与可靠性资质，保障医疗数据安全及服务持续可靠；

2）云服务应提供弹性资源与自动化支持，包括租户自服务开通与关闭、弹性计费模式选择以及基于业务负载的自动资源伸缩能力，且人工智能等技术的应用须通过科技伦理审查，并符合 GB/T 39725-2020 相关要求。

5.1.3 云原生技术兼容

a) 支持容器化部署

1) 异构环境与集群支持：应支持在多种 CPU 架构的服务器上构建 Kubernetes 集群，并支持创建包含物理机与虚拟机的混合工作负载集群；

2) 存储与加速能力：应内置分布式存储 CSI 插件，为有状态应用提供持久卷；同时应支持多种 GPU 虚拟化与共享技术，满足异构计算需求；

3) 版本与镜像管理：应支持多个标准 Kubernetes 版本，并可按需选用；应支持使用内置及私有容器镜像仓库，并可通过域名或 IP 地址向工作负载集群提供镜像服务。

b) 实现应用的快速部署、弹性伸缩和高效管理

1) 集群快速部署与治理：应支持在数分钟内快速创建 Kubernetes 工作负载集群，并具备项目级别的资源隔离与租户权限管理能力；

2) 运维可观测与高可用保障：应通过监控、告警、日志和事件等多种方式展示集群运行状态；当集群节点发生故障时，应支持自动或手动方式进行替换；

3) 节点规模弹性管理：应同时支持固定节点数量的 Worker 集群与可根据工作负载自动伸缩的弹性 Worker 集群。

5.2 异地多活部署模式

5.2.1 地理分片规则

5.2.1.1 依据患者或医疗机构地理位置划分数据归属

a) 数据归属策略基于患者常住地（通过身份证/医保卡信息）或就诊机构注册地动态划分数据归属区域，并采用 GeoHash 算法对地理位置进行编码以实现数据分片。分片原则：

1) 基于患者唯一标识划分数据归属，确保同一患者的所有数据（病历、检验、缴费）归属同一地理分片，避免跨分片查询；

2) 特殊场景处理：补充“跨区域就诊数据处理”—患者跨分片就诊时，临时生成“数据镜像” 存储于就诊地分片，就诊结束后按“主分片优先”原则同步至归属地分片，镜像数据保留 7d 后自动清理；

3) 临时跨区业务数据归属规则：明确患者因急诊转诊、异地就医等场景产生的临时数据，优先归属接诊机构所在分片，同时自动同步至原归属地分片，同步完成后标记“临时数据已归档”。

b) 本地化存储：每个地理分片对应本地数据中心，核心数据仅存储于归属地数据中心，非核心数据可跨区共享。使用分布式存储系统实现数据物理隔离，通过访问控制列表（ACL）限制跨区域数据流。

5.2.1.2 实现数据的本地化存储与访问

a) 边缘缓存加速：在区域边缘节点部署缓存服务器，缓存高频访问数据，降低跨区访问延迟；

b) 数据同步机制：采用双向异步复制 实现跨区数据一致性，冲突检测采用最后写入胜出（LWW）策略；

c) 合规性保障：通过国密 SM4 算法加密跨区传输数据，符合《中华人民共和国个人信息保护法》对患者隐私数据的本地化存储要求。

5.2.2 多数据中心协同

5.2.2.1 构建多地数据中心

a) 架构设计：本项目采用“两地三中心”或“三地五中心”架构，数据中心间通过 100Gbps 专线互联，网络延迟≤2ms。部署模块化机房以支持快速部署与弹性扩容，并通过云服务器高可用与容灾组合，实现存储双活与异地远程复制，支持灾难场景下的自动或手动切换。
b) 资源池化
   1) 计算资源：虚拟化技术，高弹性计算资源池；
   2) 存储资源：提供块、文件、对象等存储服务；
   3) 网络资源：SDN 技术实现 Overlay 网络，加强安全防护；
   4) 灾备资源：按需提供灾备服务，支持多租户自助容灾。
c) 容源池化：采用 Active-Active 双活模式，核心业务同时写入多地数据中心，RPO≤5min，RTO≤30min。

5.2.2.2 实现业务流量的灵活调度和快速切换

a) 智能流量调度：基于 GeoDNS 与全局负载均衡（GSLB），按用户地理位置、网络延迟、数据中心负载动态分配流量。集成健康检查，自动剔除故障节点；
b) 故障切换机制：部署多活控制平面，实时同步集群状态，故障时自动将流量切换至健康节点；
c) 关键业务采用无状态设计，切换期间数据差异通过日志回放同步；
d) 流量治理：基于服务网格（Istio）实现细粒度流量控制，支持金丝雀发布、熔断降级策略，故障切换时间≤200ms。

6 关键技术

6.1 混合云统一管理

包含混合云管理平台、多云适配网关、资源计量与成本管理模块、跨云配置合规检查组件、统一身份认证与权限管控组件。其中，混合云管理平台为核心枢纽，多云适配网关为跨平台交互关键，其余组件为支撑模块，形成全链路管理体系。应满足以下要求：

a) 需完全兼容 OpenStack、Kubernetes 等主流开放标准，支持国产虚拟化平台、国产操作系统及国产数据库的全生态适配，需通过国家信创安全可靠测评；
b) 具备跨云资源统一编排能力，可实现私有云、公有云、边缘节点资源的联动调度与动态扩容，支持医疗业务高峰期资源的快速调配；
c) 可视化管理界面需适配医疗机构运维习惯，提供资源状态实时监控、故障告警、报表生成等功能，支持自定义监控指标与告警阈值；
d) 权限管控需实现细粒度权限分配，支持多因素认证。

6.2 边缘节点层管理

包含轻量化边缘计算网关、本地分布式缓存节点、边缘数据同步代理、断网续传组件、边缘安全接入网关、基层终端适配接口模块。组件均采用轻量化设计，适配基层医疗机构有限的机房空间与算力资源。应满足以下要求：

a) 所有组件需支持轻量化部署，单节点资源占用（CPU≤2 核、内存≤4GB）满足基层医疗机构算力限制，启动时间不超过 3min，具备 7×24h 稳定运行能力；
b) 兼容 HL7、DICOM 等医疗行业标准协议，支持各类基层医疗终端的标准化接口适配，数据采集准确率不低于 99.9%；
c) 断网续传组件需支持断点续传与数据增量同步，可耐受连续 72h 断网场景，网络恢复后数据同步延迟不超过 5min，同步过程中不影响本地业务运行；
d) 边缘安全接入网关需支持国密 SM2、SM4 算法，具备接入身份认证、数据加密传输、入侵防御等功能，符合等保 2.0 三级要求；

e） 边缘轻量虚拟化引擎需兼容国产容器镜像，支持业务容器的快速启停与故障自愈，自愈时间不超过 1min。

6.3 私有云层管理

包含国产虚拟化平台、分布式块存储集群、私有云管理平台、国产化关系型数据库集群、中间件集群、高可用管理组件、本地灾备切换模块、专用存储节点。组件均采用国产化架构，满足信创与医疗数据安全要求。应满足以下要求：

a） 国产虚拟化平台需支持国产 CPU、国产操作系统适配，虚拟机迁移过程中业务中断时间不超过 30s，资源利用率可达到 80%以上；

b） 分布式块存储集群需满足医疗大文件高 IO 读写需求，单节点读写速率不低于 1GB/s，存储容量可横向扩展，支持存储资源动态扩容，数据可靠性不低于 99.999%；

c） 国产化数据库集群需支持 ACID 特性，兼容 SQL 标准，跨 Region 数据同步延迟不超过 3s，具备数据备份、恢复功能，恢复时间不超过 30min；

d） 中间件集群需支持高并发访问（缓存组件 QPS≥10 万，消息队列 TPS≥5 万），兼容国产软硬件生态，具备故障自愈与负载均衡能力；

e） 高可用管理组件需支持对虚拟化平台、数据库、中间件等核心组件的全面监控，故障识别延迟不超过 20s，自动恢复成功率不低于 95%；

f） 专用存储节点需支持 DICOM 标准，影像数据压缩比不低于 4:1，压缩后不影响影像质量，支持影像数据的快速检索与调阅，调阅延迟不超过 2s；

g） 所有组件需通过国家信创安全可靠测评，符合医疗数据分级保护与等保 2.0 三级要求。

6.4 全局统一调度管理

包含全局负载均衡（GSLB）设备/DNS 调度系统、跨 Region 多活调度控制器、第三方仲裁节点、数据一致性校验组件、业务优先级调度模块、跨云链路监控组件。形成“调度-仲裁-校验-监控”全闭环调度体系，保障异地多活架构稳定运行。应满足以下要求：

a） 全局负载均衡支持 HTTP、HTTPS、TCP 多协议及医疗业务会话保持，故障识别延迟≤30s、路由切换延迟≤1min；可基于 IP 归属地就近调度，结合业务优先级与资源冗余度分配流量，具备节点健康感知与故障规避能力。最优路由不可用时自动切换至备用通道，同步触发告警并记录日志。对急诊、ICU 等最高紧急度业务，优先分配低延迟链路，确保端到端延迟≤50ms；

b） 跨 Region 多活调度控制器需兼容私有云、公有云、边缘节点的资源调度协议，切换过程中保障业务数据不丢失，满足医疗业务 RPO≤5min、RTO≤1h 的高可用要求，数据中心宕机时，GLB≤5s 内切换流量，Session Persistence 保障长连接不中断；

c） 第三方仲裁节点须具备高可用性（MTBF≥100000h），投票机制具备防篡改能力，网络中断恢复后可自动同步主备中心状态，重新校准活跃节点；

d） 数据一致性校验组件需兼容医疗结构化与非结构化数据格式，校验准确率不低于 99.99%，支持校验结果可视化展示与异常数据自动告警，分布式数据库或多活存储实现实时同步，切换后自动校验数据完整性和时序一致性；

e） 业务优先级调度模块可灵活配置分级规则，支持优先级动态调整，高优先级业务资源占用优先级需高于低优先级业务，资源抢占响应时间不超过 10s；

f） 跨云链路监控组件需支持专线与 VPN 链路的双链路监控，带宽利用率阈值可自定义，丢包率超过 1%时触发告警，支持自动切换至备份链路。

6.5 跨层协同支撑

包含数据同步工具、国密加密网关、安全审计组件、云原生监控告警平台、时间同步服务器（NTP）、跨云日志管理组件。作为全架构的协同支撑体系，保障各层级、各组件之间的高效协同与安全运行。应满足以下要求：

a） 数据同步中间件，以数据同步中心模式实现同构/异构数据源间≤5s、断点续传、一致性校验的库表级实时同步；支持跨地域多机房主从、多主多从复制及国产数据库、分布式存储、医疗行业标准协议全兼容，同步失败时自动重试且重试次数可自定义。对于关系型数据库侧提供实时、异步、定时及批量同步机制并全程监控；对于非关系型数据库（Redis 等）侧支持跨数据中心

双向实时同步，通过防循环策略、缓存更新失效机制及异地多活设计。同时需要数据一致性保障机制，确保多中心场景下内存缓存与源端数据库的准实时最终一致性；

b) 国密加密网关需支持 SM2、SM3、SM4 国密算法，兼容国产网络设备与云平台，具备透明加密能力，不影响业务正常运行，支持加密流量监控与异常告警；

c) 安全审计组件需符合等保 2.0 三级与医疗数据安全管理要求，审计日志保存时间不低于 6 个月，支持日志防篡改与追溯功能，可生成合规审计报表；

d) 云原生监控告警平台需支持多维度指标采集（最低 1min/次），告警延迟≤10s，可视化展示与≥3 个月历史查询。平台统一监控多活全局负载与健康度，实时采集基础设施、业务接入、业务处理、数据存储四层指标，分层设阈值，层内/层间异常自动切换并秒级通知运维。多机制相互隔离，部分失效仍可发现重大故障，为灾难恢复提供准确实时依据，缩短决策时间，支持动态调整切换策略，平台自身高可用。支持提供开放接口，供医院方获取其所属资源的性能数据；

e) 时间同步服务器（NTP）需支持 NTPv4 协议，时间同步精度不超过 1ms，具备高可用性，支持主备部署，故障切换自动完成；

f) 跨云日志管理组件需支持多种日志格式，日志采集准确率不低于 99.9%，支持日志关联分析与全文检索，检索响应时间不超过 3s。

6.6 分布式事务框架

包含分布式事务协调器、事务日志存储节点、自动化补偿回滚引擎、并发控制模块、异常隔离存储区、事务优先级管控组件、分级告警联动模块。组件协同构建医疗专属分布式事务体系，保障跨数据中心事务一致性与业务连续性。应满足以下要求：

a) 分布式事务协调器支持基于 XA 或 TCC 模式的分布式事务处理，兼容国产分布式事务协议及主流开源协议，确保跨数据中心、多数据库操作严格遵循 ACID 特性，保障医疗业务操作原子性，规避数据不一致风险，整体分布式事务响应时间≤500ms，每秒处理能力≥100 笔；

b) 事务日志存储节点存储合规实时事务日志，为回滚/补偿操作提供数据支撑，日志需同步写入并保存≥6 个月，满足审计合规要求，同时保障日志完整性与可追溯性，适配异常场景下的数据恢复需求；

c) 自动化补偿回滚引擎基于 TCC、SAGA 等协议构建医疗业务专属体系，按诊疗环节拆分回滚单元，遵循幂等性原则，通过唯一事务 ID 标识全流程操作；遇网络中断、节点故障等异常时，依托事务日志自动执行回滚/补偿操作，快速恢复数据一致状态；

d) 并发控制模块支持乐观锁/悲观锁机制，有效解决多医生同开医嘱等医疗业务并发冲突问题，保障并发场景下的数据准确性与操作有序性；

e) 异常隔离存储区负责收纳重试失败的异常数据，对回滚失败、无法自动补偿的数据进行加密存储与标识；将异常影响限制在单个诊疗环节或患者 ID 维度，仅隔离关联事务，不影响其他患者业务处理，实现最小粒度隔离防护；同时自动触发人工干预流程（联动医院信息科运维团队），完整记录操作人员、处理时间及结果，确保全程可追溯；

f) 事务优先级管控组件支持事务重试次数差异化配置，默认自动重试≤3 次（间隔 100ms），急诊事务可调整为≤5 次；补偿策略与医疗业务优先级精准匹配，优先处理急诊等核心事务的回滚/补偿，确保 5min 内恢复可用，普通门诊事务可在 30min 内完成处理，平衡效率与安全性，重试失败后触发人工干预流程并留存完整日志；

g) 分级告警联动模块通过多活中心联动监控实时识别事务异常，触发分级告警机制，紧急告警推送至运维中台，一般告警记录于系统日志，同时自动标记异常数据所属业务单元，为故障快速处置提供支撑；

h) 业务处理层需满足无状态设计要求，各中心处理层应用相互解耦，单次处理结果及时持久化至数据存储层，处理请求仅依赖自身信息及数据存储层信息；同时保障业务处理幂等性，通过唯一事务 ID、请求校验等机制，确保同一业务请求单次执行与多次重复执行结果一致，规避重复处理导致的数据异常。

7 数据管理

在区域医疗混合云异地多活架构下，数据管理需兼顾高可用性、数据一致性、安全性与智能分析能力，确保核心业务系统连续运行，数据资源高效流动与深度利用。

7.1 数据库与数据仓库

数据库与数据仓库系统应满足高可用、高性能、高安全和高扩展性的技术要求，支撑跨数据中心核心业务系统的连续运行、数据同步以及数据分析处理能力，推动医疗数据资产的统一治理与深度应用。

7.1.1 核心业务数据库

核心业务数据库主要包括HIS、EMR、LIS、PACS及健康档案索引数据库等系统，用于支撑医疗核心诊疗、临床辅助及运营管理业务。系统需保障7×24h持续高可用，确保单点故障不影响业务运行与数据安全，并满足医疗数据完整性、一致性（跨系统同步偏差≤0.01%）和保密性要求。

7.1.1.1 采用高可用架构

应采用高可用架构，确保在部分组件或数据中心出现故障时，整体系统仍能持续提供服务，保障医疗业务的连续性。高可用架构可通过主从复制、双活集群、负载均衡和多活数据中心架构等技术手段实现。

7.1.1.2 数据备份和容灾演练

a) 备份频率要求
   1) 核心业务数据：实时增量备份，事务日志实时同步至异地备份中心；
   2) 重要数据：每日 2 次全量备份；
   3) 一般数据：每周 1 次全量备份。
b) 容灾演练要求
   1) 全业务容灾演练：每年至少 1 次；
   2) 关键系统专项演练：每季度至少 1 次。

7.1.2 数据仓库建设

7.1.2.1 数据仓库总体架构

结合 “私有云+公有云+边缘节点”混合云架构，采用异地双活数据仓库+分层存储设计，与主备数据中心协同联动，关键适配设计。要求如下：

a) 双活部署：主备数据中心均部署完整数据仓库，通过实时数据同步与一致性校验机制，避免单点故障导致服务中断；
b) 分层存储适配：敏感数据驻留于私有云分布式存储，非敏感数据按需扩展至合规公有云。边缘侧部署轻量化缓存节点，优先汇聚基础诊疗数据，并通过小时级周期同步至中心数据仓库，缓解核心链路负载。

7.1.2.2 数据仓库设计规则

a) 架构设计：采用分层模型，实现数据从原始采集到分析应用的流程化处理；基于分布式存储架构，支持海量医疗数据的高效存储与扩展；
b) 数据集成：通过 ETL 工具实现多源数据抽取、清洗和加载，确保数据一致性；
c) 安全与合规：数据加密符合 HIPAA 等法规；基于 RBAC 的访问控制，实现敏感数据脱敏；
d) 技术标准：采用医疗行业标准统一数据格式。

7.1.2.3 构建医疗数据仓库

构建适配异地多活架构的医疗专属数据仓库，实现三大目标。要求如下：

a) 数据整合：汇聚区域内医疗机构多源数据形成统一数据资产；
b) 合规安全：遵循等保 2.0、HIPAA 等要求，确保数据仓库全生命周期合规，敏感数据零泄漏；
c) 服务连续：通过主备协同、实时同步与故障自动切换机制，保障分析服务在单中心故障场景下持续可用。

7.1.2.4 支持数据分析和挖掘

a) 数据服务层建设：构建统一数据服务网关，为不同角色提供标准化数据接口，降低分析门槛；
b) 分析工具与技术集成：结合医疗分析场景需求，集成“实时分析+离线挖掘+可视化”工具链，适配混合云架构；
c) 性能优化策略：针对医疗数据量大（PB 级）、查询场景复杂（多维度聚合）特点，从存储+计算+索引三方面优化。

7.2 数据采集与交换

7.2.1 标准化数据采集

a) 遵循 WS/T 787-2021 等国家标准、行业标准确立的数据规范。
b) 支持多种数据采集方式
   1) 针对不同结构化数据，应采用数据库表、文件、网络服务（Web Service）、REST、HTTP/HTTPS、消息订阅/发布等技术进行数据采集；
   2) 对于病历等文本数据，采集过程中应结合自然语言处理等技术进行非结构化处理后采集获取；
   3) 对于智能穿戴设备、智能手机、传感器等渠道产生的类型丰富、数据量大、结构复杂的数据，应通过分布式系统接口、分布式数据流收集等技术进行数据采集；
   4) 针对由麦克风、摄像头等设备产生的海量音视频数据，应通过语音图像识别、编解码等技术转化后进行数据采集；
   5) 医疗物联网设备数据采集适配要求，明确对智能监护仪、输液泵等院内物联网设备，支持 MQTT、CoAP 协议采集，数据格式自动转换为 HL7 FHIR 标准。
c) 支持多种数据采集方法
   1) 应提供数据传输服务、高并发离线数据上传下载服务，支持 TB/PB 级别数据导入及导出；
   2) 应支持实时或定时增量数据采集；提供实时同步、定时采集、数据订阅及日志采集等服务；
   3) 应支持条件过滤进行数据采集；
   4) 应支持采集作业管理与任务调度的方法进行数据采集；
   5) 应支持数据标签，支持设置数据标记。

7.2.2 数据交换平台

7.2.2.1 建立医疗数据交换平台

a) 平台架构设计
   1) 采用分布式服务架构构建医疗数据交换平台，支持本地数据中心、公有云及异地多活节点间的跨域数据流转；
   2) 采用微服务架构，通过 API 网关统一接入，确保核心业务与非核心业务隔离传输。
b) 安全交换机制
   1) 数据传输过程中应用国密算法（SM4/SM9）实施端到端加密；
   2) 集成动态令牌认证与 RBAC 权限控制，依据角色（医生、管理员、患者）实现数据访问权限的精细化管理。
c) 高可用保障
   1) 通过全局调度层实现传输路径的智能优选，支持跨机房故障秒级切换；
   2) 内置断点续传与流量控制机制，保障大容量医疗影像等文件传输稳定性。

7.2.2.2 提高数据处理能力

a) 数据标准化处理
   1) 提供可视化映射引擎，实现非标准数据向符合 WS/T 787-2021 统一格式自动转换；
   2) 支持 HL7/FHIR 等医疗专用协议实时解析与转换。
b) 数据质量管控

1） 完整性校验：采用 SHA-256 哈希算法验证数据包完整性，传输失败时自动触发重传机制；
2） 一致性保障：通过分布式事务机制，确保跨数据中心数据交换的一致性；
3） 异常处理：实时监测传输延迟与失败率，超出阈值时自动告警并记录审计日志。

c） 业务场景适配
1） 核心业务数据：仅允许单向流出至私有云或本地数据中心，并启用动态脱敏机制；
2） 非核心业务数据：支持公有云环境下进行双向交换，并提供批量异步处理能力。

7.3 数据安全合规审计

区域医疗混合云异地多活数据中心需通过加密技术、访问控制、合规审计等手段，确保医疗敏感数据的机密性、完整性和可用性，满足国家法律法规及行业标准要求，保障患者隐私与医疗数据安全。

7.3.1 数据加密存储与传输

随着医疗数据的增长，数据安全与隐私保护已经成为医疗信息化系统中的核心问题。必须严格遵循国家关于医疗数据保护的法律法规，保障患者隐私信息不被泄漏，防止数据在传输和存储过程中遭到篡改或丢失。

7.3.2 敏感数据处理

a） 存储加密
1） 应采用字段加密和文件加密系统对存储在云中的敏感医疗数据进行加密；
2） 加密要求，对敏感字段采取字段级加密（Field-Level Encryption，FLE）；
3） 技术要求，应集成具备透明数据加密（Transparent Data Encryption，TDE）功能的数据库模块；
4） 针对医学影像文件（DICOM 格式）和电子病历文档，应采用 SM4-CBC 加密模式实施文件级加密；
5） 分布式存储系统应启用全盘加密技术。

b） 传输通道加密
1） 优先采用国密算法，传输通道加密使用 SM2/SM4（TLS 1.3+国密证书）；
2） 跨数据中心同步宜启用 SM4-GCM 模式，提供认证加密功能；
3） 面向互联网的敏感数据传输，应叠加 SM2 数字信封机制；
4） 在国际算法适配场景中，当国密算法无法实施时，应采用不低于 AES-256-GCM 认证加密模式或 RSA-3072 非对称加密算法；
5） 加密传输处理时延在万兆网络环境下应控制在 50ms 以内，通过符合 GM/T 0028-2014 标准的密码卡硬件加速模块实现。

c） 密钥管理
1） 密钥管理系统（KMS）应部署于信创环境中，主密钥（CMK）管理权限禁止委托给云服务提供商；
2） 密钥生成应采用经国家密码管理局认证的硬件密码机（HSM）或国产密码卡产生真随机数。密钥长度应符合 GM/T 0002-2012 规定的安全强度要求；
3） 主密钥应采用 PKI 分片机制，主密钥分片存储于本地 HSM 安全模块，分片密钥应通过 SM4-GCM 加密后异步复制至不少于两个地理隔离的容灾中心；
4） 业务密钥应定期轮换周期，销毁过程应符合物理销毁与逻辑擦除双重验证机制，并生成不可篡改的销毁凭证。

7.3.3 数据访问控制与审计

7.3.3.1 建立访问控制机制

a） 最小权限原则：仅授予完成职责必需的字段级权限，设置权限有效期；
b） 访问控制策略：基于 RBAC 模型细分医护、管理等角色制定细粒度策略；引入 ABAC 扩展，结合用户部门、职称等属性实现精细化管理；联动身份认证（用户名/密码、数字证书等）保障授权访问；

c） 操作日志记录：全生命周期追踪数据访问操作，记录操作时间、人员、对象、类型及源 IP、MAC 地址等关键信息；实时采集日志存储至审计数据库，定期归档与完整性校验，确保可追溯、不可篡改。

7.3.3.2 患者隐私保护

a） 动态脱敏技术：访问时实时处理敏感数据，依权限与场景对患者姓名、身份证号等隐私信息进行隐藏、加密或替换；

b） 动态脱敏规则：与访问控制策略联动，返回客户端前实时脱敏；区分场景执行差异化规则（外部研究不可逆哈希、医护查询部分屏蔽、统计分析匿名化）；建立策略管理平台，支持配置与版本管理，定期评估优化规则。

c） 特殊场景处理

1） 医学研究：开放差分隐私沙箱，允许统计分析，禁止查看个体数据，结果需通过 k-匿名性检验（每组≥5 条）；

2） 跨机构交换：采用代理重加密（PRE）技术，卫健委监管节点可解密，接收方仅见脱敏版本。

7.3.4 数据合规性管理

数据合规性管理，旨在确保医疗数据在混合云异地多活架构下的全生命周期操作合法、规范且安全。其核心要求包括严格遵循国家及地方相关法律法规，将合规要求贯穿于数据采集、存储、传输、使用、共享、销毁等各个环节。应满足以下要求：

a） 在数据采集、存储、传输、使用、共享、销毁全生命周期中，满足数据安全、隐私保护、合规操作要求，规避法律风险，保障患者权益；

b） 定期进行数据合规性评估和审查，应建立文件化数据合规性评估程序，确保数据处理持续合规。