ICS 35.240.99
CCS L60

T/GYJS

团 体 标 准

T/GYJS 014—2025

区域医疗混合云信创计算底座技术规范

Technical Specification for Regional Medical Hybrid Cloud Innovation Computing Infrastructure

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。

本文件由广州医科大学附属番禺中心医院提出。

本文件由广东省云计算应用协会归口。

本文件起草单位：广州医科大学附属番禺中心医院、广东慧云科技股份有限公司、广东省电子商务认证有限公司、广东省通信产业服务有限公司、中山大学孙逸仙纪念医院、中山大学附属第三医院、中山大学肿瘤防治中心、中山大学附属口腔医院、广州市弘宇科技有限公司、南方医科大学珠江医院、广东省第一荣军优抚医院、南方医科大学附属第三医院、广州市番禺区卫生健康局、广州医科大学附属妇女儿童医疗中心、广州医科大学附属第二医院、广州医科大学附属第五医院、广州市第一人民医院、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）、广州开发区医院、番禺区医疗卫生集团、中国医学科学院阜外医院深圳医院、深圳大学附属华南医院、深圳市第三人民医院、深圳市第四人民医院、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、深圳市龙岗区第五医院、中山市人民医院、暨南大学附属顺德医院、中山大学附属第三医院肇庆医院、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、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）、深圳市南山区医疗集团总部、粤北人民医院、连州市医疗总院、顺德区第三人民医院、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、广东飞和信息科技有限公司、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、北京志凌海纳科技股份有限公司、深圳市棒可可科技有限公司、暨南大学、西安电子科技大学、中南大学、湖南大学、北京航空航天大学、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：苏榕彬、田立明、刘化龙、张艳华、宋京、王健英、黄幸青、龙运艺、何颖新、谭建皓、力竟成、梁毅飞、林志辉、陈汉威、张泽彬、刘斌、李国练、任忠敏、吴向群、张晓东、王文辉、高峰、邹志武、张家庆、陈智斌、冯伟良、梁润锦、黄礼强、岳浩、陈树乐、宗慧、查正清、欧阳杰、任英华、徐飞、王逸欣、李鹏、陈玉兵、吴庆斌、吴庆军、何鑫波、谢显荣、李博孜、林汉辉、廖颖研、李世君、郑华国、邓意恒、韩松津、廖茂成、杨川川、李贵华、练剑锋、杨纪岚、李彬、罗雪琼、蔡永铭、郭华星、周日文、左智贤、刘昱迟、鲁俊杰、邓亚萍、陈景良、陈桂能、陈志福、张浩然、杨进、王铿、刘可儿、郑东生、王娜、雷前、张嘉鹏、苗银宾、刘志全、曾安、潘丹、杨腾飞、周望、王腾、王亮亮、林舒源、杨宝瑶、唐卓、赵伍杰、黄玉辉、王永祥、蔡勇、孙玉洁、刘玉娟、庾燕莉。

引　言

随着信息技术的飞速发展，区域医疗信息化建设不断推进，医疗数据呈现爆发式增长。根据《2022 - 2023 年中国信创生态及信创 PC 市场发展研究报告》，信创产业作为国家战略的重要组成部分，其发展对于保障国家信息安全、推动经济数字化转型具有重要意义。在医疗领域，构建一个稳定、可靠、符合信创要求的混合云计算底座，已成为提升区域医疗信息化水平、保障医疗数据安全的关键举措。

目前，国内医疗行业在云计算应用方面虽有一定基础，但在混合云架构下，特别是在信创环境下的计算底座技术规范尚未完善，导致各区域医疗云平台建设标准不一，数据共享与协同困难，系统稳定性与安全性难以保障。本项目旨在制定一套完整、科学、可操作的区域医疗混合云信创计算底座技术规范，涵盖架构设计、硬件选型、软件部署、数据管理、安全防护、性能优化等方面，为区域医疗云平台建设提供标准化指导，确保其满足信创要求，实现自主可控、安全可信、高效可用。

区域医疗混合云信创计算底座技术规范

1 范围

本文件规定了区域医疗混合云环境下信创计算底座的模型、技术架构和通用技术要求，适用于医疗信息系统国产化替代、自主可控云平台建设及医疗数据安全治理。

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 18894-2016 电子文件归档与电子档案管理规范
GB/T 20945-2013 信息安全技术 信息系统安全审计产品技术要求和测试评价方法
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 29765 2021 信息安全技术 数据备份与恢复产品技术要求与测试评价方法
GB/T 31167-2023 信息安全技术 云计算服务安全指南
GB/T 31168-2023 信息安全技术 云计算服务安全能力要求
GB/T 31496-2023 信息安全技术 信息安全管理体系指南
GB/T 31500-2024 网络安全技术 存储介质数据恢复服务安全规范
GB/T 32399-2024 信息技术 云计算 参考架构
GB/T 37964-2019 信息安全技术 个人信息去标识化指南
GB/T 38542 2020 信息安全技术 基于生物特征识别的移动智能终端身份鉴别技术框架
GB/T 39477-2020 信息安全技术 政务信息共享 数据安全技术要求
GB/T 39725-2020 信息安全技术 健康医疗数据安全指南

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 Medical Hybrid Cloud
整合公有云与私有云资源，为区域内医疗卫生机构提供计算、存储、网络及安全服务分布式云平台。

3.2

信创计算底座 Innovation-oriented Computing Infrastructure
基于国产化处理器、操作系统及数据库构建的云计算基础设施，实现软硬件的自主可控与混合云协同管理，支持医疗业务系统的无缝迁移与异构资源统一调度。信息技术应用创新产业，其计算底座作为支撑数字化转型的国产化基础设施，其核心特点是全栈自主、安全可信、集约高效和生态聚合。

3.3

医疗数据脱敏 Medical Data Desensitization
通过技术手段对医疗健康数据中的敏感信息进行变形或屏蔽，确保数据可用性与隐私安全的平衡。

3.4

云边协同 Cloud-Edge Collaboration
云计算中心与边缘计算节点之间的资源调度、数据互通及服务协同机制。

3.5

细粒度访问控制 Fine-grained Access Control

对用户访问权限进行最小化和分级控制，在字段、记录、接口、操作行为等维度上提供权限的精细化管理。

3.6

访问控制策略 Access Control Policy

定义主体访问资源时所需满足的授权规则和条件。

3.7

数据审计 Data Auditing

系统对数据访问和操作全过程进行记录、存储、分析及追踪的过程，确保行为可追溯、责任可查。

3.8

不可抵赖性 Non-repudiation

防止操作主体事后否认行为发生的安全特性，通常依赖时间戳、数字签名等技术手段。

3.9

访问控制模型 Access Control Model

用于实施访问控制的框架包括：基于角色的访问控制、基于属性的访问控制、基于策略的访问控制。

3.10

自主可控 Autonomous Controllability

通过国产化芯片、操作系统、数据库等核心组件的技术替代，实现信息技术产业链关键环节的安全可控，降低外部依赖风险。

3.11

云原生架构 Cloud-Native Architecture

基于微服务、容器化及DevOps等技术构建的分布式系统架构，支持医疗应用的弹性扩缩容、持续集成与跨平台部署。

3.12

信创适配验证 Innovation-oriented Adaptation Verification

针对国产化软硬件环境兼容性测试与性能调优流程，涵盖功能测试、安全测评及供应链合规性审查。

3.13

零感知迁移 Zero-Perception Migration

在整个迁移过程中，无需修改源代码、保持原有交互习惯的前提下完成系统迁移，终端用户和在线业务对切换动作“毫无察觉”，即服务不中断、性能不下降、数据不丢失、操作习惯无需改变。

4 缩略语

下列缩略语适用于本文件。

SAML：安全断言标记语言（Security Assertion Markup Language）

SM2/SM3/SM4：国家密码管理局发布的商用密码算法，其中 SM2 为非对称密码算法，SM3 为密码杂凑算法，SM4 为对称密码算法。

FHIR：快速医疗互操作资源（Fast Healthcare Interoperability Resources）

MFA：支持多因素身份认证（Multi-factor Authentication）

MTBF：平均无故障时间（Mean Time Between Failure）

RBAC：基于角色的访问控制（Role-Based Access Control）

5 信创计算底座模型

区域医疗混合云信创计算底座是基于国产化处理器、操作系统及数据库等核心组件构建的云计算基础设施，整合公有云与私有云资源，形成“云-边-端”协同的分布式云平台（如图1）。其核心特征体

现为全栈自主可控、安全可信、高效可用、兼容适配及可扩展，旨在为区域内医疗卫生机构提供计算、存储、网络、安全及应用支撑等一体化服务，实现医疗业务系统无缝迁移、异构资源统一调度与医疗数据全生命周期安全治理，最终支撑区域医疗信息化国产化替代、数据共享协同及服务效率提升，满足信创产业 “2+8+N”推进体系中医疗行业逐步完成信创改造的战略要求。

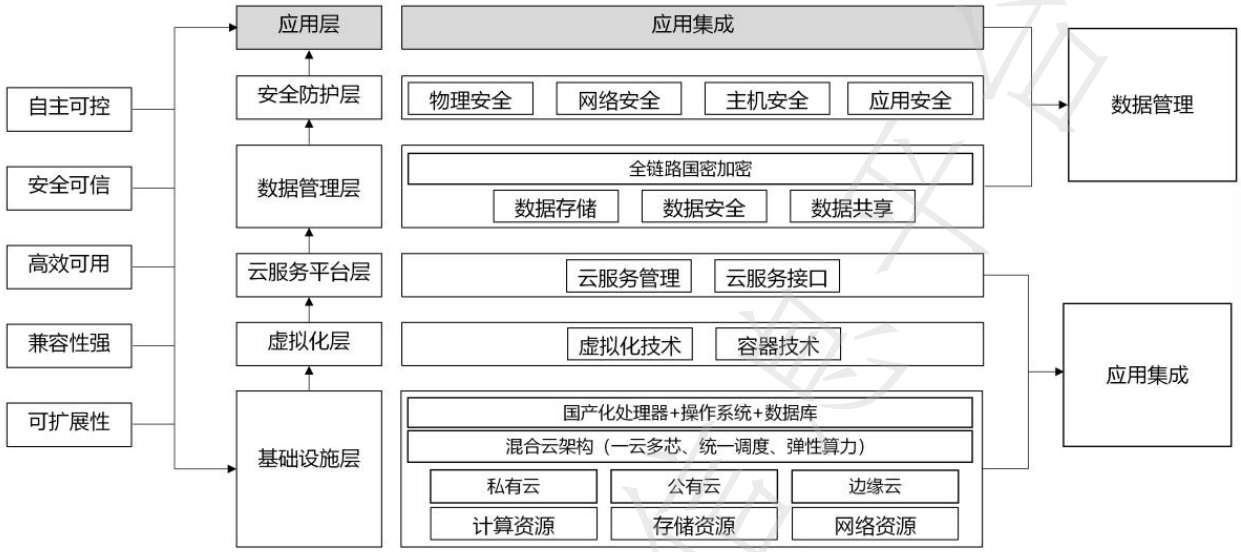

图1　区域医疗混合云信创计算底座模型

6　总体架构设计

6.1　基础设施层

6.1.1　计算资源

a）　硬件选型：应采用通过中国信息安全测评的国产化服务器硬件，能够适配多种 CPU 架构，确保硬件的兼容性和稳定性；
b）　性能要求：计算资源应具备高性能处理能力，适配多核处理器、高性能 GPU 等硬件，满足区域医疗业务的高并发需求；
c）　扩展性：具备横向和纵向扩展，以适应业务增长的需求，确保系统的可扩展性。具备高密度计算和虚拟化扩展，单节点物理 CPU 核心数不低于 32 核；内存容量可扩展至 TB 级，具备 ECC 错误校验；存储需兼容 NVMe 协议，单机存储带宽≥10Gbps。

6.1.2　存储资源

a）　存储类型：能适配多种存储类型，包括 SSD、HDD 等，满足不同数据类型的存储需求；
b）　数据保护：提供数据备份和恢复功能，确保数据的安全性和一致性。具备全量备份、增量备份和差异备份；
c）　性能优化：优化存储性能，提高数据读写速度，能够大数据量的存储和访问。具备多控架构，控制器节点数量可线性扩展，单控制器故障应实现业务无感知的自动切换。

6.1.3　网络资源

a）　网络架构：应采用高速稳定的虚拟化网络技术以提升资源利用率。核心设备应基于自主设计的国产芯片及国产操作系统，从硬件层面实现自主可控，且芯片须通过安全测评。设备需兼容 SDN、OpenFlow 等通用协议，支持流量动态调度、业务快速部署及跨域集中管理，满足医疗业务灵活调整需求；同时应兼容国产云平台混合云管理接口及云原生编排协议，适配“一云多芯”异构算力环境，保障医疗核心业务在混合云中稳定运行；
b）　安全隔离：通过虚拟局域网（VLAN）等技术，实现不同业务系统的网络隔离，确保网络安全；
c）　带宽管理：采用动态带宽调整技术，根据业务需求合理分配网络资源；

d) 区域医疗混合云数据中心应采用 VXLAN、M-LAG、EVPN 等虚拟化网络技术及微服务适配能力，构建跨物理边界、高可靠的大二层组网架构，以满足多院区协同与业务灵活扩展的需求。

6.2 虚拟化层

6.2.1 虚拟化技术

a) 虚拟化平台：应优先采用国产化自主可控的虚拟化平台，兼容多种虚拟化技术，兼容主流国产 CPU 架构，兼容多种国产操作系统、数据库。以满足异构环境下的资源管理与业务部署需求，依托技术特性实现高效、稳定的虚拟化支撑；
b) 资源管理：提供灵活的资源管理功能，具备资源的动态分配和回收。具备虚拟机生命周期管理、资源动态调度、高可用热迁移、数据备份与恢复等核心功能；
c) 性能优化：优化虚拟化性能，减少虚拟化开销，提高系统的整体性能。具备在线扩容与负载均衡，满足医疗业务高峰期对计算资源弹性需求，性能表现匹配区域医疗混合云的业务负载特征。

6.2.2 容器技术

a) 容器平台应采用国产化自主可控，提供容器化应用的部署与管理功能；
b) 微服务架构应具备支撑应用开发、部署与运维的能力，保障应用的可扩展性与可维护性；
c) 容器安全应提供容器安全防护功能，确保容器环境的安全性。

6.3 云服务平台层

6.3.1 云服务管理

提供丰富的云服务目录，兼容多种云服务模型。

6.3.2 云服务接口

a) 需遵循国家标准与行业标准，兼容 RESTful API、SOAP API 等常用接口协议；接口参数、返回值格式需统一，提供详细的接口文档（包含调用示例、错误码说明），降低集成难度；
b) 提供 API 管理功能，具备 API 的注册、认证、授权与监控能力，能与各类医疗信息系统的集成与互操作；能与区域医疗现有信息系统的集成，通过标准化接口实现数据同步与业务协同；能够与上级医疗平台的对接，实现数据上报与资源共享；
c) 具备服务编排功能，实现复杂业务流程的自动化部署和管理；
d) 需采用身份认证、数据加密（国密 SM4 算法）机制，确保接口调用的安全性；同时具备接口调用监控功能，可实时监控接口调用量、响应时间、错误率，当接口出现异常时自动告警，保障接口稳定运行。

6.4 数据管理层

a) 数据存储：存储应采用具备高可用与可扩展性的分布式架构，并提供数据备份与恢复功能。备份机制须支持全量、增量及差异备份，恢复功能应包括快速恢复与灾难恢复能力；
b) 数据安全：应采用加密技术保障数据在存储与传输中的安全，并兼容多种加密算法。同时须提供细粒度访问控制与数据审计功能，确保访问权限可控，并完整记录数据访问及操作日志以支持事后追溯；
c) 数据共享：应建立区域医疗数据共享平台，支持医疗机构间的数据共享与业务协同。平台需提供安全可靠的数据交换功能，实现异构系统间数据交互，并具备数据治理能力，保障数据质量与一致性。

6.5 安全防护层

a) 物理安全：机房环境应符合国家标准，保障设备物理安全；须采取防静电、防雷击及防火等措施，确保设备安全运行；同时应建立严格的人员管理制度，控制机房访问权限；
b) 网络安全：应部署高性能防火墙以提供网络边界防护，采用入侵检测系统实时监测网络攻击，并配置 DDoS 防护机制确保网络服务的高可用性；
c) 主机安全：主机应采用国产操作系统，并建立漏洞管理机制以实时发现与修复系统漏洞。同时应对主机实施安全加固，提升系统的整体抗攻击能力；

d) 应用安全：应部署应用防火墙以提供应用层防护，对应用代码实施安全审计，并在上线前完成全面的安全测试，确保应用系统的安全性；
e) 应用集成：系统应具备与其它医疗信息系统的集成能力，通过提供标准化接口规范实现互操作，并支持安全可靠的数据交换功能，以促进跨系统数据交互与共享，支撑业务协同。

7 通用技术要求

7.1 自主可控

区域医疗信息系统安全可信的底座平台，确保关键基础设施不受外部制约、可持续演进。

7.1.1 硬件选型

硬件选型是区域医疗混合云信创计算底座技术架构的基础，涉及服务器、存储、网络等多个层面的设备选择。选型标准应根据国产化要求、性能需求、扩展性及可靠性来进行，确保硬件平台能够支撑医疗行业对高可用、高性能和高安全性的数据处理需求。

7.1.1.1 选型原则

采用“合规选型标准 + 场景化验证 + 分阶段实施”的实施路径，以合规优先、稳定可靠、适配协同、医疗适用为核心原则，确保国产化硬件全面符合信创政策标准，并有效支撑区域医疗混合云信创计算底座及异地多活场景的核心运行需求。要求如下：

a) 合规优先：硬件产品须通过国家权威机构安全可靠测评，或纳入省级信创产品适配目录/医疗信创生态认证清单，且在有效期内；符合网络安全等级保护三级要求及医疗信创建设相关指南规范；
b) 稳定可靠：硬件 MTBF≥1 万小时；核心部件（电源、风扇）采用冗余架构设计；硬件故障恢复时间≤1h；
c) 适配协同：兼容主流国产操作系统、国产数据库及中间件；
d) 医疗适用：具备医疗数据高并发处理能力及大带宽传输性能；支持国密加密算法，满足医疗数据加密存储与传输要求。

7.1.1.2 分设备国产化选型标准

a) 服务器应实现全栈自主可控：核心芯片须采用国内自主指令集架构，完成设计、流片、封测全流程；固件应由国产厂商开发，支持国密算法数字签名，并提供关键源代码可查；操作系统宜预装通过自主可控测评的国产服务器版本，确保内核无境外闭源组件并兼容医疗数据库。禁止使用国外授权架构芯片及非自主操作系统；
b) 存储设备应实现“协议-加密-控制芯片”自主可控。其核心硬件（主控芯片、缓存控制器、加密单元等）须采用国产自主方案，不得依赖境外专用 ASIC 或 FPGA，并能提供完整供应链溯源信息与芯片自主知识产权证书。固件及管理软件栈（包括固件擎、数据服务模块、加密模块与管理平台等）均须在国内自主研发，代码自主可控，能在纯国产环境中全功能运行；设备应可在断网环境下独立完成部署、配置与故障恢复，确保无境外 License 或云服务依赖；
c) 网络与安全设备应实现全栈自主可控。其核心硬件（交换芯片、防火墙芯片、通信模块等）须采用国产方案并提供自主知识产权证明，能在断网环境下满负载稳定运行。系统应搭载基于国产 OS 的固件，主流网络协议须自主研发，通过抓包与代码审查验证无境外私有协议或未授权开源依赖。安全功能须基于国产规则引擎，威胁情报与策略库支持本地化更新与演练，确保不依赖境外云端服务、License 或心跳连接；
d) 网络与安全设备在混合云架构下的选型应满足以下要求：核心硬件（交换芯片、防火墙芯片等）须为国产自主可控产品，提供自主知识产权证明，并适配国产虚拟化及云管理平台，确保在混合云环境中稳定协同运行。云间网络与控制面应自主研发，支持国产密码算法加密，东西向与南北向流量策略须由本地管理平面独立配置，通过抓包验证协议无境外私有字段，并确保跨云数据同步的完整与安全。安全防护须基于国内自主训练的规则库，支持全域策略联动，通过混合云环境攻击模拟测试防护效能，并核查无境外威胁情报依赖及调用行为；
e) 云管理与运维应使用国产自主可控混合云管理平台，支持信创设备统一纳管、资源调度与监控，提供标准化运维接口且无境外技术依赖。需验证平台对信创设备的全生命周期管理能力，核查其国产化认证，确保运维操作无境外组件调用。

7.1.1.3 适配验证体系

为避免“选型即锁定、部署即不兼容”的实施风险，须构建覆盖全生命周期的国产化硬件适配验证体系，以标准化测试驱动选型决策，确保硬件在具备生态兼容、功能完整、运行稳定、安全可控的一体化集成能力。要求如下：

a) 标准符合性测试：验证硬件是否通过国家信创权威机构的兼容性认证；确认其对主流信创 CPU、操作系统、云平台等基础生态组件的官方支持清单有效性，未通过认证或无实测报告者不进行采购；
b) 功能互操作测试：在实验室环境中，验证硬件与 HIS、PACS 等关键系统的 API、协议、驱动及管理接口的互通能力；重点检查是否存在私有协议依赖、闭源驱动绑定或境外 License 校验机制；
c) 场景压力与高可用测试：模拟真实医疗业务负载，在混合云典型拓扑（含边缘节点、异地灾备）下开展高负载、断网自治、故障切换等压力测试，验证硬件在极端工况下的服务连续性与恢复能力；
d) 安全合规性测试：委托具备资质的第三方机构，对硬件固件、驱动、管理模块开展代码成分分析、国密算法实现验证、信创评测及后门检测；确保加密、日志、访问控制等安全功能完全本地化，无境外威胁情报或远程心跳依赖；
e) 持续兼容性保障：建立管控机制，确保后续固件或驱动更新不影响现有系统兼容性，并纳入厂商服务承诺，防范长期运维中的生态断裂风险。

7.1.1.4 确保硬件的自主可控

混合云信创基础设施硬件自主可控聚焦“芯片-固件-供应链-运维”全链条管控。核心要求如下：

a) 全栈自主选型：优先采用“自主架构芯片+国产固件+国产 OS”全栈方案，杜绝境外核心依赖的伪自主模式；核心硬件组件须具备国产自主知识产权，供应链可追溯，严禁使用含未公开指令集或安全后门的产品；
b) 合规验证保障：通过供应链追溯核查、断网运行测试、国密及等保认证等手段强化自主可控验证；须通过国家级信创适配认证及主流国产软硬件互认证，兼容医疗行业标准协议硬件加速需求；
c) 资源管控适配：支持多架构服务器混合部署，依托虚拟化或容器化技术实现资源统一调度；
d) 运维与效能要求：搭建国产化运维工具链，组建本地化团队实现全生命周期自主管控；核心硬件自主可控率≥95%、供应链境外依赖度≤5%，筑牢敏感数据安全屏障。

7.1.2 软件选型

7.1.2.1 国产操作系统

应优先选用基于Linux内核、适配“一云多芯”架构自主可控操作系统，建议采用通过中国信息安全测评中心认证的“国产自主可控操作系统”。选型时应评估其与医疗行业主流应用软件、国产数据库及中间件的兼容性，并验证与虚拟化层、容器层的适配能力，确保全栈架构稳定运行。

操作系统应满足硬件层“等保三级物理安全”延伸要求，提供不低于网络安全等级保护三级的安全加固能力，包括强制访问控制、内核级安全审计、漏洞快速修复机制，且能够通过标准API接入多云管理平台，实现与“跨云资源池统一调度”架构的协同，满足医疗数据高安全性与资源自动化运维需求。

7.1.2.2 国产数据库

应选用具备自主知识产权、适配国产芯片生态的数据库系统，宜选用国产自主可控操作系统。数据库应支持分布式架构与弹性扩展，以应对医疗业务高峰期的海量并发访问，同时应兼容虚拟化层部署与容器层容器化部署，符合“一云多芯”架构的资源调度要求。

应严格遵循GB/T 39725-2020要求，提供数据加密存储（含敏感医疗数据分级加密）、传输加密及脱敏功能；容灾能力应覆盖“同城双活、异地灾备”，保障电子病历、检查报告等核心数据的连续性与一致性。此外，应与国产操作系统深度融合优化，确保软件栈性能匹配医疗PaaS服务的运行需求。

7.1.2.3 国产中间件

应选用适配“一云多芯”架构、支撑医疗混合云应用的国产中间件，宜选用国产自主可控中间件。中间件应承担服务层核心枢纽作用，提供高可用的应用服务器、消息队列（支撑影像数据跨云传输）、

API网关（对接医疗PaaS服务接口）及分布式事务协调功能，保障跨虚拟化平台、跨容器集群部署应用的可靠通信。

应具备完善的标准兼容性，全面兼容Java EE、微服务架构及医疗行业开发框架，确保现有HIS、PACS系统平滑迁移与新建影像AI应用快速部署；内置安全管控模块应与云平台身份认证系统集成，实现服务认证、授权与安全审计，同时应满足硬件层“等保三级”延伸的应用安全要求，保障电子病历调用、患者信息查询等敏感操作合规性。

7.1.2.4 确保软件的自主可控

所有基础软件选型应遵循技术自主可控与安全可信原则，以实现“一云多芯”全栈自主可控目标。要求如下：

a) 知识产权与供应链保障：所选软件应具备完整自主知识产权，供应商应纳入工信部信创工委会名录，确保极端情况下技术服务连续性与供应链安全；
b) 全栈适配认证：应建立覆盖“芯片—操作系统—数据库—中间件—虚拟化—容器”的国产化适配认证体系，所有软件应通过第三方机构的安全漏洞扫描、代码自主率评估，且应验证与硬件层国产服务器、存储设备的兼容性；
c) 风险管控：严禁使用未公开源代码、存在后门或高危漏洞的软件，应重点排查虚拟化层、容器层的兼容风险；
d) 数据主权保障：应通过“国产自主可控操作系统+国产中间件”的全栈架构，实现从硬件层到服务层的全链路自主可控，保障区域医疗健康数据的安全存储与合规使用，符合“跨云资源池统一调度”中的数据主权要求。

7.2 安全可信

7.2.1 数据加密

a) 数据加密技术：应构建符合国家密码管理要求的加密技术体系。具体包括采用国家认可的对称加密算法，以满足海量医疗数据的高速加密需求；应用合规的非对称加密技术，以保障密钥安全分发与数字签名的可靠性；并运用国家标准的杂凑算法，确保数据完整性得到有效验证；
b) 数据全流程加密规范：数据在存储和传输过程中应实施全流程加密防护。存储环节需对数据库执行字段级加密、对分布式存储执行卷级加密，并对备份数据强制加密；传输环节要求网络传输使用 TLS 1.3 及以上协议，跨系统交换须通过 IPSec VPN 加密通道，所有 API 接口调用必须启用 HTTPS 并实现双向认证；
c) 算法选用原则：应遵循国密算法优先原则，在信创环境中以国密算法为主体，仅在必要场景下兼容国际算法。具体要求为核心业务系统须强制采用 SM2/SM3/SM4 国密算法套件；在异构系统交互等必要场景下，可辅以 AES-256、RSA-2048 等国际算法。所使用的密码模块应通过国家密码管理局检测认证，并具备国产密码硬件加速能力。

7.2.2 访问控制

a) 细粒度的访问控制功能：访问控制策略应满足 GB/T 39725-2020 及相关法律法规要求，明确权限范围并细化终端设备控制。应依据信息密级划分安全域，部署边界防护设备，实施流量过滤与安全检测并定期审查完善。在合规前提下，可借助缓存、负载均衡等技术优化访问性能、降低延迟。须完整记录所有访问与操作日志，实现行为可追溯与安全审计，并对日志进行归类分析以识别风险、改进策略。审计日志应受保护，确保其完整、可靠与防篡改；
b) 数据的访问权限可控：权限管理应符合 GB/T 39477-2020 中关于授权管理的规定，并基于用户角色和实际需求对医疗数据进行精确的访问控制。应实现数据权限的分级管理，建立定期审查与更新机制，确保权限设置的准确性与有效性。同时，应明确医疗大数据在采集、存储及使用各环节的规范与限制，切实保护患者隐私与信息安全；
c) 具备基于角色的访问控制：在应用最小权限原则时，应基于职责与需求实施精确授权，遵循权限分离与最小特权要求，确保用户或系统仅获取执行任务所必需的最低权限。系统默认执行最小权限，额外权限须经特别申请。需定期审查并更新权限设置，及时撤销不必要的权限。同时，须完整记录与监控用户及系统活动，以便及时发现异常行为与安全事件并采取应对措施。

7.2.3 身份认证

7.2.3.1 多种身份认证方式

身份认证应支持基础口令与 X.509 数字证书两种主要方式，并可采用生物识别作为辅助验证，且所有认证过程应记录完整日志，支持审计与追溯。具体应符合以下要求：

a) 口令认证：系统默认采用用户名及口令方式，密码须以 SM3 加随机盐值加密存储，强制有效期不超过 90d。连续登录失败超过 5 次应锁定账户至少 30min，并提供安全的密码找回机制。严禁账户共用，确保操作可追溯至自然人；
b) 证书认证：应支持基于 X.509 标准的数字证书，兼容国产 PKI 体系及 SM2 算法。建立完整证书信任链验证机制，支持 CRL（证书撤销列表）和 OCSP（在线证书状态协议）检查，确保证书有效。数字证书可存储于智能卡、USB Key 等硬件安全模块，并与用户账号强制绑定，确保身份准确识别。应提供证书到期前 30d 自动提醒及更新功能，支持证书透明度日志记录；
c) 生物识别：生物特征数据须在本地存储，禁止原始数据上传云端，并确保与个人账号唯一绑定，杜绝特征共用。

7.2.3.2 用户身份的真实性

在区域医疗混合云信创计算底座的设计与实现过程中，确保用户身份的真实性是保障数据安全、业务合规和防范非法访问的核心环节。医疗系统涉及大量敏感信息，因此，必须通过严格的身份认证机制确保只有合法用户可以访问系统，防止未授权用户的入侵和身份伪造。具体应符合以下要求：

a) 系统应支持并实施多因素认证（MFA）。须集成多种认证方式，对所有涉及敏感操作的系统访问强制启用 MFA，确保仅合法身份用户可执行操作。认证机制应包括动态口令及基于硬件设备的身份验证，以有效防范静态密码泄漏风险；
b) 系统应支持指纹、人脸等生物识别技术，适用于门禁控制、医生工作站登录及患者自助终端等场景，以增强身份验证的便捷性与唯一性。可在终端、门禁及自助设备中集成智能识别模块，通过实时比对确保用户身份真实性；
c) 系统应支持实时身份验证与行为分析。每次用户访问均需进行实时验证，并根据访问频次、时间及操作行为动态调整认证强度。应结合 AI 与机器学习技术，分析用户常规行为特征，实现动态身份评估与异常行为检测，一旦发现异常自动触发重新验证并报警。系统可根据用户角色、访问级别及环境智能调整认证策略，以降低身份伪造与滥用风险；
d) 身份认证防伪机制应通过动态认证协议与加密通道防止中间人攻击与身份伪造，确保信息传输安全。系统须采用严格的账户锁定、多重验证及访问时段与 IP 地址限制，防止账号滥用与共享。同时应为管理员提供完整的审计与日志记录功能，确保所有操作可追溯；
e) 所有身份认证操作应进行完整日志记录，并通过专门审计系统实施定期安全审查。当检测到身份认证异常时，系统须自动触发预警，立即采取临时锁定账户、强化验证或通知管理员等响应措施，以阻断安全风险扩散。

7.2.3.3 统一的身份认证平台

应支持医疗行业多角色身份全生命周期管理，涵盖用户名、工号、所属机构、岗位权限等核心信息建档，实现同一用户在HIS、PACS、EMR等核心业务系统中的身份唯一标识映射，避免多账号冗余。同时，应依据用户角色和访问场景配置差异化认证强度，高权限角色应启用多因素认证，普通角色可按需选择单因素或双因素认证。

在认证协议兼容性上，应全面支持SAML 2.0、OAuth 2.0、OpenID Connect 1.0等主流协议，确保与现有及新建医疗应用无缝对接；还应支持SM9等国产自主认证协议，可对接UKey、智能卡等国产密码设备，且应能通过标准API接入医保、政务等第三方认证服务，实现跨领域身份互认。权限控制应采用RBAC模型，支持自定义医疗业务角色并关联细粒度权限，同时应具备权限继承与隔离机制，防止越权访问。

7.2.3.4 SSO 功能

7.2.3.4.1 协议与认证要求

a) 单点登录（SSO）应基于 OAuth 2.0 与 OpenID Connect 协议族实现，并采用国密 SM2/SM3 算法进行数字签名与令牌加密，同时兼容 SAML 2.0 协议以对接非标准医疗系统；

b) 单点登录的国密安全增强要求包括：令牌（Token）须采用 SM4-GCM 加密且签名密钥由 HSM 托管，同时认证过程须强制实施双因素验证（用户名/密码+国密 UKey 或生物特征）。

7.2.3.4.2 安全控制机制

a) 实时风控：异常位置登录自动阻断并告警；单账号并发会话数≤1 防止账号共享；
b) 会话管理：各系统\终端最长持续 2h 自动失效；高危操作触发二次认证；
c) 审计溯源：记录完整登录轨迹（时间、IP、设备指纹、访问系统）；审计日志经 SM3 哈希后存入区块链防篡改。

7.3 高效可用

7.3.1 高性能计算

7.3.1.1 高性能的网络计算资源

a) 资源构成：应基于异构计算架构，集成多架构 CPU（ARM/LoongArch/X86）及 GPU/NPU/FPGA/ASIC 等加速卡，以支撑医疗影像、基因测序等高算力负载。同时需采用分布式内存架构，实现节点间带宽≥392GB/s、延迟≤1μs 的低延迟数据交互；
b) 资源调度：应基于 Kubernetes 构建弹性调度框架，支持动态资源分配与负载均衡，确保任务队列响应时间≤5ms。同时需集成 Slurm、PBS 或 SGE 等作业调度系统，支持优先级队列与抢占式调度机制，保障关键医疗业务的优先执行。

7.3.1.2 支持多核处理器、高性能 GPU 等硬件

a) 多核优化：启用 NUMA 架构优化，绑定计算任务至特定 CPU 节点，减少跨节点通信开销。支持 OpenMP、MPI 混合并行编程模型，最大化利用多核 CPU 资源；
b) GPU 加速：部署 GPU Direct RDMA 技术，实现 GPU-GPU 直连通信，带宽≥392GB/s。支持 MindSpore、PyTorch 等框架，模型推理吞吐量≥10k images/s。

7.3.1.3 满足区域医疗业务的高并发需求

a) 分布式架构：采用微服务架构，服务间通信通过 gRPC 协议实现，单节点并发连接数≥10 万。集成集群缓存热点数据，缓存命中率≥99.5%；
b) 容灾与弹性扩展：支持 KVM 虚拟机动态迁移，故障切换时间≤200ms。基于 Prometheus+Alertmanager 实现资源使用率监控，阈值告警响应时间≤1min。

7.3.2 高性能存储

7.3.2.1 高性能的存储资源

应存储虚拟化组件应支持冷热数据分层、I/O 本地化、RDMA 无损网络及 SPDK-vhost 加速技术，并提供分布式存储功能以池化集群内服务器的本地硬盘。数据访问须支持基于负载均衡与主备切换的多路径机制，确保存储节点故障时业务可自动切换，保障服务连续性。

7.3.2.2 满足不同数据类型的存储需求

医疗混合云依据业务场景的存储性能需求，提供差异化存储服务。要求如下：
a) 对数据库等实时关键业务，采用集中式存储保障极致性能；
b) 对 HIS、EMR 等核心系统，提供高性能块存储以满足高 IO 访问；
c) 对 PACS 海量影像文件，支持文件/对象存储，通过标准接口实现高效共享与成本优化；
d) 对门户、OA 等一般业务，提供分级块存储，平衡性能与成本；
e) 对长期保留的冷数据，集成机械盘、固态盘及蓝光存储，通过统一存储空间实现。

7.3.2.3 数据的高可用性和容错机制

a) 区域医疗混合云平台中的数据存储系统应具备高可用性设计，确保在单点故障或局部资源失效时，数据服务不中断；
b) 存储系统宜采用冗余配置机制，包括但不限于多副本存储、RAID（Redundant Array of Independent Disks）、分布式副本、纠删码等，以实现数据的快速恢复与持续可用；

c) 数据存储服务应支持自动故障检测与修复机制，在节点异常时能够自动迁移数据副本，保障业务连续性；
d) 存储架构应支持横向扩展能力，在扩展过程中不影响已有业务系统的数据可用性和一致性；
e) 为提升整体系统鲁棒性，平台可集成分布式一致性协议来协调多节点数据状态，确保在网络抖动或部分节点故障时系统仍能维持一致性服务。

7.3.2.4 数据的持久性和一致性

为确保区域医疗关键业务数据的完整性与可靠性，系统应实现跨层级的数据持久性、一致性及合规性保障。具体如下：

a) 数据持久性与容灾：基于国产分布式存储，采用多副本与纠删码冗余架构，实现跨机柜/跨机房数据分布，确保单点故障下数据零丢失，持久性不低于 99%。应建立同城双活或异地三中心容灾体系，满足相关灾难恢复规范要求；
b) 事务一致性机制：核心业务系统须基于国产分布式数据库的 Raft/Paxos（分布式共识算法）协议实现强一致性事务，确保写入后立即可见。非核心业务可采用最终一致性模型，通过版本向量保证数据收敛。所有事务应支持 ACID 特性，并在异常时自动触发补偿，故障恢复时间控制在 30s 内；
c) 合规性设计与验证：医疗数据存储年限须满足 30 年法定要求，采用 WORM（单写多读）存储模式防篡改。所有数据操作需实时生成国密 SM3 哈希指纹，并同步至国产区块链平台存证。技术实现须兼容国产芯片架构，对大文件实施分段校验，并通过一致性测试框架验证异常场景下的数据可靠性，符合相关监管要求。

7.3.2.5 支持分布式存储和集中式存储的混合使用

在区域医疗混合云架构中，需支持分布式存储与集中式存储的混合使用，需根据数据的特性、访问频率、安全合规要求以及业务场景，灵活地部署和管理数据。对于实时响应速度要求最快的数据库类型或对业务双活有强诉求的服务，建议采用集中式存储方式部署，对于通常类型的业务访问，可采用分布式存储部署。

7.3.3 高性能网络

网络交换机需满足区域医疗业务高峰时并发需求，保障医学影像、电子病历等大流量业务顺畅传输。

7.3.3.1 高性能的网络资源

a) 网络架构：采用 CLOS 无阻塞拓扑，核心交换机支持 400G 端口速率，支持 RoCE，交换容量≥900Tbps。包转发率≥200,000Mpps；
b) 存储网络：分布式存储网络，支持 NVMe over Fabrics（NVMe-oF）协议，存储节点间带宽≥100Gbps，IOPS≥1M。

7.3.3.2 支持万兆以太网、InfiniBand 等高速网络技术

a) 协议支持：原生支持 RoCEv2 或 InfiniBand，实现 RDMA 无损传输，端到端延迟≤10μs。兼容 TCP/IP 协议栈，支持零拷贝技术，减少 CPU 协议栈开销；
b) 硬件加速：采用国产高性能芯片，通过硬件加速处理 VXLAN 封装解封装操作，减少对设备运行的性能损耗，提升虚拟化网络场景下的处理效率；
c) 流量调度：基于 P4 可编程交换机实现动态流量调度，支持 ECMP（等价多路径）与智能路由。集成流量整形与 QoS 策略，保障医疗数据优先传输。

7.3.3.3 满足区域医疗业务的高带宽需求

a) 带宽保障：网络带宽应满足核心层≥40Tbps、汇聚层≥10Tbps、接入层≥1Tbps 的要求，支持 100GE/400GE 端口，并通过流量镜像与 NetFlow 分析实现实时监控与拥塞预警，预警准确率不低于 99%。宜采用 M-LAG 技术实现端口聚合、链路备份与带宽叠加，支持故障自动切换、多速率端口自适应及多设备统一管理。应基于 QoS 等协议对医疗业务流量进行分类标记与优先级保障，确保关键业务在网络拥堵时优先传输，并配置充足缓存以应对突发流量，避免数据丢失与业务中断；

b) 性能优化：启用 RDMA over Converged Ethernet（RoCE），减少 CPU 协议处理开销，带宽利用率提升至 95%。支持网络功能虚拟化（NFV），动态调整网络切片带宽分配。

7.4 兼容性强

a) 硬件兼容性：计算底座应保证在国产化硬件生命周期内，异构部件替换或扩容时业务不中断，且性能衰减不超过 5%；
b) 软件兼容性：计算底座应确保医疗核心业务系统在国产化软件栈上可部署、可运行、可升级，且升级后兼容性不降低；
c) 应用兼容性：计算底座应支持医疗核心业务系统在“零感知”至“可控改造”范围内平滑迁移，确保业务功能完整、性能可预测、中断时间可控。

7.5 可扩展性

7.5.1 架构设计

a) 采用模块化设计：虚拟化平台应提供基于 KVM 的计算虚拟化，支持 CPU、内存及 GPU 虚拟化；提供自研分布式存储，支持 2 副本、3 副本及纠删码冗余策略；提供网络虚拟化，支持分布式交换机、虚拟网络及 LLDP（链路层发现协议）；并提供虚拟分布式防火墙，支持基于标签、安全组及 IP 组的东西向流量访问控制安全策略；
b) 方便未来进行升级和扩展：平台应支持计算与存储资源的在线升级及扩展，并允许在同一集群内扩展配置异构的服务器设备（包括不同代际 CPU、不同数量与容量的 SSD/HDD）。同时，应以集群或虚拟机为单位配置 CPU 兼容指令集，至少支持最近三代以内的指令集兼容性；
c) 适应区域医疗信息化发展的需求：支平台应同时提供虚拟机与容器形态的计算资源，并支持 X86、C86、ARM 及 LoongArch 等多种架构芯片。

7.5.2 资源扩展

7.5.2.1 支持计算资源、存储资源和网络资源的动态扩展

区域医疗混合云信创技术底座应支持计算资源、存储资源和网络资源的动态扩展。动态资源扩展指对云主机而言（如果前期配置资源vCPU、vMEM）不充足或者随着业务量的增加导致原有资源紧张），通过DRX（动态资源扩展）功能自动扩充云主机的资源，以保证业务的持续运行。

动态扩展实现逻辑：平台实时监控业务云主机CPU、内存等计算资源消耗，当消耗达到自定义阈值时，校验云主机所在物理节点剩余资源。若节点资源充足，将在不中断业务的前提下为云主机追加vCPU、vMEM资源；若节点资源不足，则暂停资源调整，规避对同主机其他业务的影响。

7.5.2.2 确保系统能够根据业务需求进行弹性伸缩

区域医疗混合云信创技术底座需支持弹性伸缩服务，依据自定义策略自动调整伸缩组内计算资源，实现业务高负载扩容、低负载缩容。与云负载均衡联动，自动增减vAD实例中对应云主机，为潮汐式医疗业务提供最优资源供给。核心功能流程如下：

a) 伸缩组归集同类无状态业务实例，作为策略执行基础单元；
b) 配置扩容/缩容/告警触发阈值，支持定时与资源告警两类策略；
c) 系统同步配置并持续监控阈值指标，触发后执行对应动作；
d) 扩容时基于预设模板启动实例，纳入负载均衡节点池承接业务；
e) 调度新增连接至新节点，启动冷却机制避免重复伸缩浪费。

附 录 A
（资料性）
区域医疗混合云信创计算底座典型配置

A.1 基础设施层——国产化算力与混合云架构融合

a) 应构建基于国产芯片与信创服务器的算力底座，集成高密度算力，通过软件定义数据中心技术实现计算与存储资源池化与动态调度，满足医疗影像处理、PB 级数据处理等高负载需求；
b) 应采用分层云架构：核心业务部署于私有云，基于信创超融合架构保障高可用；非敏感业务部署于公有云，实现轻量化部署；边缘节点用于数据缓存与物联网实时交互；
c) 网络与安全架构应实现基于国密算法的跨云加密互联，部署下一代防火墙及入侵检测系统，遵循安全分区、横向隔离、纵向认证策略。

A.2 平台层——信创生态与智能能力集成

a) 应构建以国产操作系统、数据库及中间件为基础的信创软件栈，确保系统平滑迁移，支撑高并发事务处理，并集成低代码平台以加速应用开发；
b) 应建设智能能力中台，通过本地化部署医疗大模型与数据治理平台，实现临床辅助决策效率提升 25%以上，支撑疾病模型构建与慢病管理标准化。

A.3 应用层——场景化医疗服务与数据共享

a) 应基于 HL7 FHIR 等标准实现电子病历跨机构共享与全域调阅，构建覆盖预约、AI 辅助诊断、远程会诊的智能诊疗闭环，缩短患者就医时间 30%；
b) 应建立覆盖市-县-街-村的四级数据通道，实现区域检验检查结果互认，降低基层误诊率，并构建基于混合云架构的应急指挥与传染病监测预警平台。

A.4 分布式存储架构

应构建高可用、可扩展的分布式存储架构，支撑多类型医疗数据的高效访问，并适配混合云环境。具体要求包括应具备横向扩展与动态调度能力；通过冗余与隔离技术保障数据持续可用；支持分级存储与数据优化；适配国产 CPU 与软件，对关键数据实施国密加密存储与安全流转。

A.5 数据安全与合规体系

a) 应实施覆盖采集、传输、存储、使用、销毁全生命周期的安全防护，包括国密算法传输加密、分布式加密存储与区块链存证、动态脱敏及合规的数据销毁；
b) 应建立基于“两地三中心”架构的双活容灾体系，实现核心业务 RTO≤4h，并通过远程镜像与异步复制保障业务连续性。

A.6 运维与管理体系

a) 应建设统一运维平台，实现跨云资源监控、AI 日志分析与自动告警，安全事件响应时间≤15min，并支持基于 Kubernetes 的容器化部署、灰度发布与分钟级扩容；
b) 应采用“一云多芯”平台支持混合架构与在线迁移，迁移过程性能下降≤3%，并为中小医疗机构提供“等保云服务”模式以降低初期投入。

A.7 政策合规与生态协同

该模型通过全栈国产化与混合云融合，在保障数据安全合规的前提下，可提升医疗服务效率与基层能力，患者满意度可达 92%，形成可复制的医疗信创转型路径。未来应持续关注隐私计算、联邦学习等技术，破解跨机构数据融合与 AI 训练的合规难题。

附 录 B
（资料性）
接口合规检查项

在区域医疗混合云信创计算底座的建设中，接口规范是实现“云-边-端”协同、跨系统互操作、数据安全流转及信创组件兼容的核心支撑，应围绕“功能适配、安全合规、医疗特性、信创兼容”四大核心目标构建。结合行业实践、医疗数据特性及信创要求，其接口规范可拆解为以下五大核心维度，各维度下包含具体的接口定义、技术要求及应用场景。

B.1 基础设施层接口规范应实现资源统一调度与信创硬件适配

基础设施层接口规范应符合以下要求：

a) 计算资源接口须遵循国家信创硬件接口标准，兼容主流混合云平台管理接口，支持虚拟机与容器的全生命周期管理及资源状态实时监控；
b) 存储资源接口应支持对象存储（S3 协议）和块存储（iSCSI 协议），且信创存储设备须符合 GB/T 31500-2024；
c) 网络资源接口需遵循软件定义网络（SDN）标准，支持基于 VLAN 的网络隔离、动态带宽分配与安全组策略管理，并全面兼容 IPv6 协议。

B.2 数据交互层接口规范应实现保障医疗数据安全与标准流转

数据交互层接口规范应符合以下要求：

a) 医疗数据交换接口应优先采用 FHIR R4 标准并兼容 HL7 v2.x 协议，传输过程须启用 TLS 1.3 加密，并基于 OAuth 2.0 或 OpenID Connect 进行身份认证；
b) 数据脱敏接口须遵循 GB/T 37964-2019，支持部分掩码、假名化等处理技术，并输出具备可追溯标识的脱敏数据；
c) 数据同步接口须支持 CDC 与断点续传，完整记录同步日志，且符合国家备份恢复安全要求。

B.3 应用支撑层接口规范应支持跨系统兼容与信创生态适配

应用支撑层接口规范应符合以下要求：

a) 应用部署接口须支持基于容器标准与信创系统包管理接口（RPM/DEB）自动化部署与灰度发布；
b) 服务调用接口应基于微服务架构，其中医保接口需符合国家医保平台规范，AI 模型接口应兼容 ONNX Runtime 以适配信创 AI 芯片；
c) 监控告警接口应支持通过 Prometheus API 进行指标采集，兼容 Grafana API 实现可视化，并提供符合安全要求的多渠道告警推送功能。

B.4 安全管控层接口规范应构建医疗数据全链路安全屏障

信安全管控层接口规范应符合网络安全等级保护三级及以上要求，具体如下：

a) 身份认证接口须支持基于 GB/T 38542-2020 多因素认证（MFA），并兼容统一身份认证（单点登录 SSO），实现“一次登录、多系统访问”；
b) 权限控制接口应遵循基于角色的访问控制（RBAC）模型，支持角色与权限的动态管理，并将数据访问控制细化至字段级别；
c) 安全审计接口须完整记录操作人、时间、操作内容及 IP 地址四要素日志，符合 GB/T 20945-2013，并提供日志导出功能。

B.5 信创适配层接口规范应保障国产化组件兼容与替代

信创适配层接口规范应确保国产化组件与传统系统兼容性，实现平滑迁移与功能无损。要求如下：

a) 硬件适配接口须遵循信创驱动标准，确保芯片及设备与驱动的兼容性，并支持 USB 3.0、DICOM 3.0 等关键外设接口，实现非信创医疗设备与信创存储系统的安全对接；
b) 软件适配接口应提供 API 兼容层，支持非信创软件向信创操作系统迁移；其数据库适配接口须兼容 JDBC/ODBC 等标准协议，保障传统数据库系统向国产数据库的无损迁移与业务连续性。

附 录 C
（资料性）
医疗数据分级保护实施要求

数据管理应遵循“分类分级、生命周期全覆盖、安全合规、高效共享”的原则，支撑区域医疗业务连续性与数据主权要求。

C.1 法律依据

本附录依据《中华人民共和国数据安全法》第21条、《中华人民共和国个人信息保护法》第51条、GB/T 39725-2020及《卫生健康行业数据分类分级指南（试行）》制定。

C.2 医疗数据五级划分

表 C.1 医疗数据分级与保护基线

序号	级别	数据示例	泄漏影响	RPO	RTO	加密算法	访问控制	审计频率
1	5 极敏感	基因、HIV、孕产史	极高	≤15s	≤5min	SM4-硬件	字段级+多因素	实时
2	4 核心	电子病历全文、DICOM	高	≤15s	≤5min	SM4-卷级	表级 RBAC	每小时
3	3 重要	住院首页、处方	中	≤1h	≤15min	SM4-文件	角色级	每日
4	2 内部	匿名化统计	低	≤24h	≤2h	可选 TLS1.3	角色级	每周
5	1 公开	医院简介	无	—	—	无	只读	每月

C.3 数据生命周期管理

a) 采集：源系统通过国密 TLS 1.3 通道接入，支持 OAuth 2.0 双向认证；
b) 存储：核心数据采用多副本+纠删码，副本跨机房、跨地域分布；持久性 ≥ 99.9999 %；
c) 使用：敏感字段实时脱敏，支持部分掩码、假名化，脱敏算法可审计；
d) 共享：通过 FHIR R4 标准接口实现跨机构共享，传输过程端到端加密；
e) 归档：≥ 30 年长期保存，采用 WORM（单写多读） 存储+区块链指纹，防止篡改；
f) 销毁：过期数据执行物理粉碎或符合 GB/T 18894-2016的逻辑擦除，生成不可恢复证明。