ICS#

WS

中 华 人 民 共 和 国 卫 生 行 业 标 准

WS/T XXXXX—XXXX

区域医疗协同业务应用子平台技术规范

Technical specification for regional medical collaborative business application sub platform

（征求意见稿）

－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国国家卫生和计划生育委员会#
发 布

目　　次

区域医疗协同业务应用子平台技术规范

1 范围

本标准规定了区域医疗协同业务应用子平台的总体框架、技术框架、基本功能要求、信息资源规范、安全规范等关键技术要求，定义了区域医疗协同业务应用子平台的 IT 基础设施规范、机构接入规范和性能要求。本标准不包括基于区域医疗协同业务应用子平台的应用系统（如远程会诊、远程影像诊断、远程心电诊断、远程病理诊断、区域医学检验、区域消毒供应、双向转诊、远程培训等）。

本标准适用于区域医疗协同业务应用子平台的建设，以及相关医疗卫生机构对区域医疗协同业务应用子平台的接入。

区域卫生信息平台的核心目标是建立全国统一的居民电子健康档案，核心建设内容是健康档案的信息架构，数据归集是以患者结果性诊疗信息为主；医院信息平台是以电子病历为核心，重点解决医院内部不同业务系统之间实现统一集成、资源整合及以患者为中心的医疗机构内跨异构信息系统的医疗信息共享和业务协同问题，医院信息平台集成数据既包含出院患者的结果性诊疗信息，又包含在院患者的过程性诊疗信息；因此，区域卫生信息平台和医院信息平台都难以满足区域内各级医疗机构之间开展双向转诊、代理检验和远程医疗等业务需求，区域医疗协同业务应用子平台遵照国家卫生计生委的相关标准规范，通过在医院前置服务器部署区域医疗协同数据资料整合服务，实现医院信息系统内部数据的标准化转换并完成数据上传，以保证数据的标准性、完整性、安全性，为区域医疗协同服务和医疗协同业务监管提供数据支撑和业务协同，满足多级不同医疗机构之间开展区域医疗协同服务需求，实现统一的区域医疗协同服务功能应用。

区域医疗协同业务应用子平台主要包括三种区域医疗协同服务模式：一是区域内多级医疗机构之间纵向医疗协同服务模式，以区域内大型综合性医院为核心，与本区域内二级医院、一级医院和社区卫生服务中心等开展的区域医疗协同服务；二是同级医疗机构之间建立的横向医疗协同服务模式，如区域内大型医疗机构之间在医疗业务和诊疗技术方面开展的医疗协同服务；三是异地不同等级医疗机构之间远程医疗协同服务模式。

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，仅所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。

《基于电子病历的医院信息平台技术规范》（WS/T 447-2014，2014-05-30）

《基于居民健康档案的区域卫生信息平台技术规范》（WS/T 448-2014，2014-05-30）

《卫生信息数据元目录》（WS 363-2011,2011-08-02）

《卫生信息数据元值域代码》（WS 364-2011,2011-08-02）

《城乡居民健康档案基本数据集》（WS 365-2011,2011-08-02）

《电子病历基本数据集》（WS 445-2014，2014-05-30）

《卫生信息基本数据集》系列（WS 370-375,2012）

《卫生信息共享文档规范（征求意见稿）》（2012-04-28）

《居民健康卡技术规范》（2011-07-04）

《健康档案基本架构与数据标准》（2009-05-19）

《电子病历基本架构与数据标准》（2009-12-31）

HL7，卫生信息交换标准（Health Level 7）

IHE，(Integration Healthcare Enterprise，集成医疗企业) 集成规范

DICOM，医学数字影像和通讯标准（Digital Imaging and COmmunication of Medicine）

ICD-9/ICD-10，国际疾病分类（International Classification of Diseases,ICD）

3 术语、定义和缩写语

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

DICOM3.0：医学数字影像和通信标准（Digital Imaging and Communications in Medicine）

PACS：图像归档和通信系统（Picture Achieving and Communication System）

PC：个人计算机（Personal Computer）

EMR：电子病历（Electronic Medical Record）

EHR：电子健康档案（Electronic Health Record）

3G：第三代移动通信系统(The Third Generation)

AD：目录服务器(Active Directory)

ADSL：非对称数字用户线路(Asymmetric Digital Subscriber Line)

ALG：应用层网关(Application Level Gateway)

APN: 接入点名称(Access Point Name)

AS: 自治系统(Autonomous System)

BE: 数据节点(Back End)

BFCP：资源管理协议（Binary Floor Control Protocol）

BFD: 双向转发检测(Bidirectional Forwarding)

BGP: 边界网关协议(Border Gateway Protocol)

CCD: 电荷耦合器件(Charge Coupled Device)

CIDR: 无类别域间路由(Classless Inter-Domain Routing)

CIF: 标准图像格式，支持 352×288 分辨率(Common Intermediate Format)

CPU: 中央处理器(Central Processing Unit)

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

Diff-Serv: 有差别服务(Differentiated Service)

DMZ: 半信任区(Demilitarized Zone)

DNS: 域名服务器(Domain Name Server)

EGP: 外部网关协议(Exterior Gateway Protocol)

FCoE: 以太网光纤通道(Fibre Channel over Ethernet)

FCP: 光纤通道协议(Fibre Channel Protocol)

FRR: 快速重路由(Fast Reroute)

FTP: 文件传输协议(File Transfer Protocol)

GK: 网守(Gatekeeper)

GR: 优雅重启(Graceful Restart)

GW: 网关(Gate Way)

HA: 高可靠性(High Availability)

H-QoS: 层次化 QoS(Hierarchical Quality of Service)

HTTP: 超文本传输协议(Hypertext Transfer Protocol)

HTTPS: 超文本传输安全协议(Hypertext Transfer Protocol Secure)

ICMP: 因特网控制报文协议(Internet Control Message Protocol)

IDS: 入侵检测系统(Intrusion Detection System)

IGP: 内部网关协议(Interior Gateway Protocol)

IOPS: 每秒进行读写操作的次数(Input/Output Operations per Second)

IP: 互联网协议(Internet Protocol)

IPS: 入侵防御系统(Intrusion Prevention System)

IPsec: 因特网协议安全协议(Internet Protocol Security)

iSCSI: 因特网小型计算机系统接口(Internet SCSI)

ISDN: 综合业务数字网(Integrated Services Digital Network)

IS-IS: 中间系统到中间系统(Intermediate System to Intermediate System)

ISP: 因特网服务提供方(Internet Service Provider)

I-SPF: 增量路由计算(Incremental Shortest Path First)

ITU: 国际电信联盟(International Telecommunications Union)

ITU-T: 国际电信联盟－电信部分(International Telecommunications Union-Telecommunication)

LCD: 液晶显示器(Liquid Crystal Display)

LDAP: 轻型目录访问协议(Lightweight Directory Access Protocol)

LSA: 链路状态公告(Link State Advertisement)

LUN: 逻辑单元号(Logical Unit Number)

MAC: 消息鉴别码(Message Authentication Code)

MPLS: 多协议标记交换(Multiprotocol Label Switching)

MTBF: 平均故障间隔时间(Mean Time Between Failures)

MTTR: 平均修复时间(Mean Time to Repair)

NAT: 网络地址转换(Network Address Translation)

NBU: 网络备份服务器(NetBackup)

NDMP: 网络数据管理协议(Network Data Management Protocol)

NGN: 下一代网络(Next Generation Network)

NSR: 不间断路由(Non-Stop Routing)

OA: 办公自动化(Office Automation)

OSPF: 开放式最短路径优先(Open Shortest Path First)

PHB: 逐跳行为(per-hop behavior)

PoE: 以太网供电(Power Over Ethernet)

PRC: 部分路由计算(Partial Route Calculation)

PSTN: 公用交换电话网(Public Switched Telephone Network)

QoS: 服务质量(Quality Of Service)

RADIUS: 一种远程 AAA 拨号服务(Remote Authentication Dial-In User Service)

RAID: 独立磁盘冗余阵列(Redundant Array of Independent Disks)

RIP: 路由信息协议(Routing Information Protocol)

RP: 路由执行器(Route Processor)

RPO: 以恢复点为目标(Recovery Point Objective)

RTCP: 实时传输控制协议(Real-time Transfer Control Protocol)

RTP: 实时传输协议(Real-time Transfer Protocol)

SAS: 串行连接的 SCSI(serial attached SCSI)

SATA: 串行的 ATA(Serial Advanced Technology Attachment)

SCSI: 小型计算机系统接口(Small Computer System Interface)

SDH: 同步数字体系(Synchronous Digital Hierarchy)

SEC: 超强纠错(Supper Error Concealment)

SLA: 服务水平协议(Service Level Agreement)

SMC: 业务管理中心(Service Management Center)

SMI-S: 存储管理主动规范(Storage Management Initiative - Specification)

SNMP: 简单网络管理协议(Simple Network Management)

SOAP:简单对象访问协议(Simple Object Access Protocol)

SPC: 存储程序控制(Stored Program Control)

SPI: 同步并行接口(Synchronous Parallel Interface)

SRTP：安全实时传输协议(Secure Real-time Transport Protocol)

SSD: 固态磁盘(Solid-State Drive)

SSH: 安全外壳(Secure Shell)

SSL: 安全套接层(Secure Sockets Layer)

TCP：传输控制协议(Transmission Control Protocol)

TE：远程呈现终端(Telepresence Endpoint)

TLS：传输层安全(Transport Layer Security)

UCD：用户为中心的设计(User Centered Design)

UDP：用户数据报协议(User Datagram Protocol)

VOIP GW：宽带语音网关(Voice over Internet Protocol Gate Way)

VPN：虚拟专用网(Virtual Private Network)

VRRP：虚拟路由冗余协议(Virtual Router Redundancy Protocol)

VSS：虚拟软件交换机(Virtual Software Switch)

WAN：广域网(Wide Area Network)

XML：可扩展标记语言(Extensible Markup Language)

4 区域医疗协同业务应用子平台框架及建设要求

4.1 总体框架

区域医疗协同业务应用子平台的总体框架主要包括标准规范体系、安全保障体系、网络硬件基础设施、运维服务体系、基于区域医疗协同业务应用子平台的应用、区域医疗协同业务应用子平台的服务、信息资源中心，如图 1 所示。

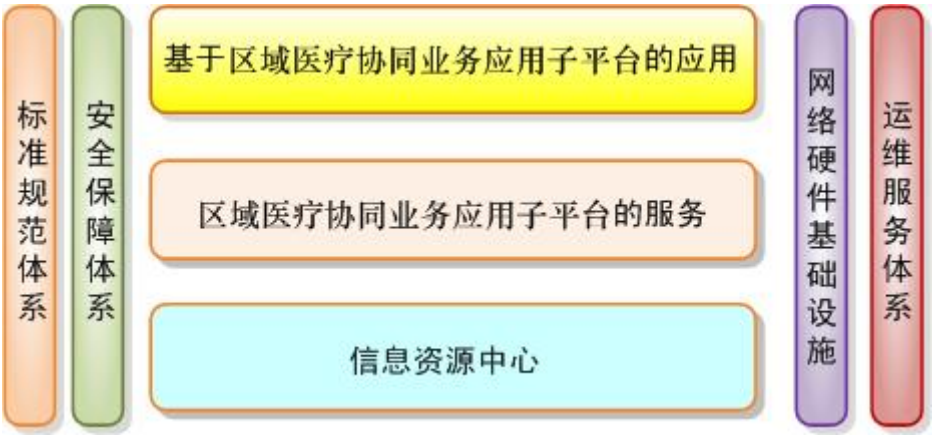

图 1 区域医疗协同业务应用子平台总体框架

4.2 技术架构

区域医疗协同业务应用子平台技术架构是从技术方面进行分层和描述，核心部分是区域医疗协同业务应用子平台及基于区域医疗协同业务应用子平台的应用系统。区域医疗协同业务应用子平台的技术架

构包括五个层次，即应用层、服务层、资源层、交换层、接入层。如图 2 所示。

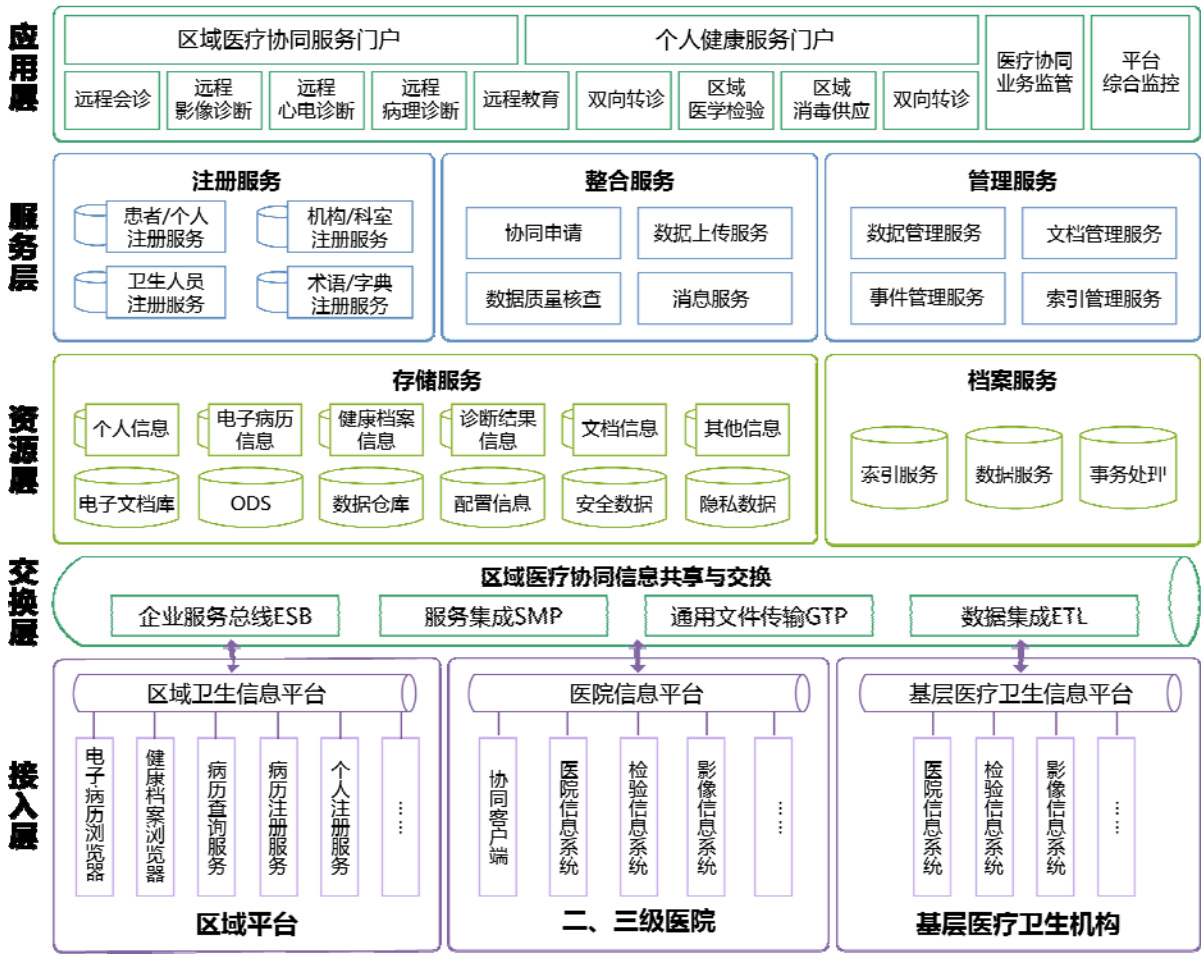

图 2 区域医疗协同业务应用子平台技术架构

4.2.1 应用层

区域医疗协同业务应用子平台应用层是在区域医疗协同和信息整合的基础上，按平台规范进行开发，调用平台上的各种信息资源和服务，结合实际业务需求建立的扩展应用。例如区域医疗协同、居民健康卡、电子病历浏览器、管理辅助决策支持系统、平台综合监控系统等。

4.2.2 服务层

区域医疗协同业务应用子平台服务层所提供的服务包括注册服务、区域医疗协同服务、区域医疗协同数据资料的整合服务、管理服务、存储服务和调阅服务。服务层为区域医疗协同服务、远程医疗服务、医疗协同业务监管及平台运行维护提供服务支持，各类服务之间通过消息交换和消息传输贯穿，服务间的消息交换基于通用的交换标准和行业的交换标准。

4.2.3 资源层

区域医疗协同业务应用子平台资源层所提供资源包括结构化数据、非结构化数据、结构化文档数据、应用服务资源等。资源层主要为区域医疗协同工作开展的管理协调、功能建设以及辅助决策开展数据统计分析服务，为各级区域医疗协同中心之间的互通互联提供信息服务。

4.2.4 交换层

区域医疗协同业务应用子平台交换层主要用于满足跨地区、跨医疗机构的信息交换和业务协同。交换层根据区域医疗协同实际业务流程，通过数据接口或消息传递方式，在平台与平台之间、平台与区域医疗协同业务系统之间进行数据集成与交换，实现信息共享。

4.2.5 接入层

区域医疗协同业务应用子平台接入层包括区域卫生信息平台、医院信息平台及基层医疗卫生信息平台，它是开展区域医疗协同业务应用的基础。

4.2.5.1 区域卫生信息平台

区域医疗协同业务应用子平台与区域卫生信息平台实现互通互联。对于已经建设区域卫生信息平台的省市，区域医疗协同业务应用子平台是区域卫生信息平台的补充，患者/个人信息、机构/科室信息、专家信息及术语/字典信息是调用区域卫生信息平台上已注册的信息，调用区域卫生信息平台上已有的健康档案信息和电子病历信息。

4.2.5.2 医院信息平台

区域医疗协同业务应用子平台与医院信息平台或基层医疗卫生信息平台对接，将通过平台机制，实现医疗机构之间的信息共享和医疗协同，减少数据接口数量。如果医疗机构未建设医院信息平台，区域医疗协同业务应用子平台与医院信息系统的对接。

4.3 建设要求

4.3.1 软件架构要求

基本要求包括：

——平台架构应基于面向服务架构的思想来构建，采用基于 XML 的数据交换技术和基于 Web 服务的数据交换技术；

——平台应支持“热插拔”集成，服务请求者与服务提供者是松散耦合关系，应用系统遵循数据规则和相应接口，即可集成到平台中，实现与其他应用系统的交互；

——平台架构应支持基于数据驱动的消息传输机制，支持消息主动发送、请求/应答、订阅/发布三

种消息交换模式；

——平台架构要求具有消息路由功能，根据最终目的地自动解析网络路径，实现数据的多步、多级传输，可以具有业务流程管理（BPM）。

4.3.2 管理功能要求

基本要求包括：

——平台提供管理和监管工具，能够对区域医疗协同业务应用进行管理和监督，支持数据预警、消息提醒等智能化服务；

——平台支持统一身份认证和集成权限管理，支持数据防篡改和隐私数据保密，支持业务流程追溯和审计等；

——平台具备较强的扩展性，支持基于平台的二次应用开发；

——平台基于企业服务总线 ESB 实现区域医疗协同服务注册、申请、审核、集成和服务监控等功能，服务默认采用 Web Service 方式。

4.3.3 交互信息要求

交互信息应支持 WS 363-2011、WS 364-2011 等国家颁布的相关卫生数据标准，参考国际卫生行业相关数据标准。

5 基本功能和交易规范

5.1 注册服务

注册服务用于区域医疗协同业务应用子平台各种共享服务资源的注册，通过服务资源的发布－发现－访问机制，实现服务资源共享。注册服务是医疗协同信息闭环系统中基础服务之一。

注册服务包括对患者/个人、医疗卫生人员、专家、医疗卫生机构（科室），术语和字典的注册管理服务，系统对这些实体提供唯一的标识。

5.1.1 个人注册服务

个人注册服务用于对医疗协同服务的患者基本信息进行管理。通过对个人基本信息的统一管理，实现对个人信息最完整的保存，可以为区域医疗协同业务应用子平台上的各应用系统提供一致的个人信息。基本功能要求包括：

——具备新增个人注册功能；

——具备个人信息更新功能；

——具备个人身份失效功能；

——具备个人身份合并功能；

——具备个人信息查询功能；

——基本信息发生修改后，平台主动发送消息到相关的目的系统。

5.1.2 医疗卫生人员注册服务

医疗卫生服务人员注册用于对医疗单位内部所有医疗卫生服务人员的基本信息进行注册和管理。医疗卫生服务人员包括医生、护士、医技人员等提供医疗卫生服务的所有医务人员，通过对医疗卫生服务人员基本信息、专业信息的记录，可以实现对医疗卫生服务人力资源的全面掌控、统一管理、合理配置。基本功能要求包括：

——具备新增医护人员注册功能；

——具备医护人员更新功能；

——具备医护人员失效功能；

——具备医护人员查询功能；

——基本信息发生修改后，平台主动发送消息到相关的目的系统。

5.1.3 医疗卫生机构（科室）注册服务

医疗卫生机构（科室）注册用于医疗卫生机构（科室）的基本信息管理。通过对医疗卫生机构（科室）基本信息的统一管理，可以为区域医疗协同业务应用子平台上的各应用系统、患者提供完整、统一的医疗机构（科室）信息。基本功能要求包括：

——具备新增医疗卫生机构（科室）注册功能；

——具备医疗卫生机构（科室）更新功能；

——具备医疗卫生机构（科室）停用功能；

——具备医疗卫生机构（科室）查询功能；

——信息发生修改后，平台主动发送消息到相关的目的系统。

5.1.4 专家注册服务

专家注册用于对医疗机构外部提供医疗协同服务专家的职称、特长等信息进行注册管理。专家注册服务以医疗卫生人员注册服务为基础，对已注册的医疗卫生服务人员中的专家特定信息进行补充。通过

对专家基本信息的统一管理，可以为区域医疗协同业务应用子平台上的各应用系统和患者提供完整、统一的专家信息。基本功能要求包括：

——具备新增专家信息注册功能；

——具备专家信息更新功能；

——具备专家信息失效功能；

——具备专家信息查询功能；

——基本信息发生修改后，平台主动发送消息到相关的目的系统。

5.1.5 术语和字典注册服务

术语注册用于从数据定义层来解决各系统的互操作问题。术语的范围包括医疗卫生领域所涉及到的各类专业词汇，以及所遵循的数据标准。建立术语和字典注册库，用来规范医疗卫生事件中所产生的信息含义的一致性。术语可由平台管理者进行注册、更新维护；字典既可由平台管理者又可由机构内各应用系统来提供注册、更新维护。基本功能要求包括：

——具备术语和字典的注册功能；

——具备术语和字典的更新功能；

——具备术语和字典的查询功能；

——具备术语和字典的版本管理功能；

——具备向应用系统同步术语和字典功能。

5.2 区域医疗协同数据资料整合服务

区域医疗协同数据资料整合服务提供对区域医疗协同数据资料的采集整合处理能力，包括区域医疗协同申请信息接收服务（远程医疗申请单信息、双向转诊申请单信息、区域医学检验申请单信息）、区域医疗协同数据资料上传接收服务、区域医疗协同数据质量核查服务、区域医疗协同数据资料上传查询服务及区域医疗协同申请信息查询服务。

5.2.1 区域医疗协同申请信息接收服务

区域医疗协同申请信息接收服务用于对区域医疗协同应用系统发出的各种申请信息的接收、校验、存储，基本功能要求包括：

——具备区域医疗协同申请单信息接收功能；

——具备区域医疗协同申请单信息校验功能；

——具备区域医疗协同申请单信息存储功能。

5.2.1.1 角色和交易

区域医疗协同申请信息接收服务主要有两类角色参与，分别为区域医疗协同申请信息源和区域医疗协同申请信息接收服务组件，由区域医疗协同申请信息源向区域医疗协同申请信息接收服务组件发送申请，具体如图 3 所示。

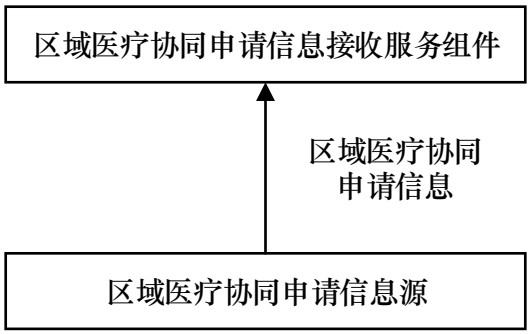

图 3 区域医疗协同申请信息接收服务角色交易图

5.2.1.2 角色交易选择

角色交易的选择，如表 1 所示。

表 1 区域医疗协同申请信息接收服务角色—交易关系表

角色	交易	选择
区域医疗协同申请信息源	申请区域医疗协同	应有
区域医疗协同申请信息接收服务组件	申请区域医疗协同	应有

5.2.1.3 交易流程

区域医疗协同申请信息接收服务的基本流程，如图 4 所示。

——区域医疗协同申请信息源发送区域医疗协同申请信息到区域医疗协同申请信息接收服务组件；

——区域医疗协同申请信息接收服务组件接收区域医疗协同申请信息后效验数据并存储。

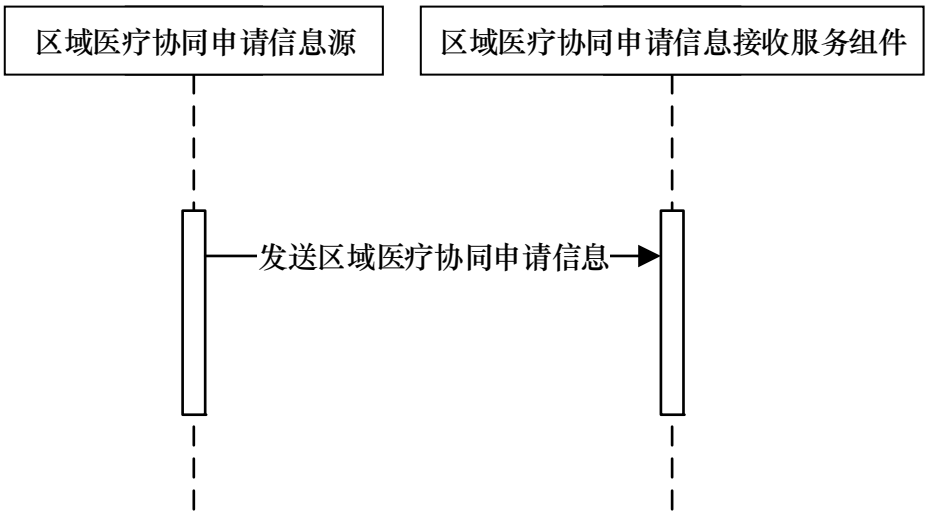

图 4 区域医疗协同申请信息接收服务时序图

5.2.2 区域医疗协同数据资料上传接收服务

区域医疗协同数据资料上传接收服务用于区域医疗协同各类应用系统上传的数据资料的接收、检验、存储等，如远程医疗数据资料、双向转诊数据资料、区域医学检验数据资料等数据资料，基本功能要求包括：

——具备区域医疗协同数据资料接收功能；

——具备区域医疗协同数据资料校验功能；

——具备区域医疗协同数据资料存储功能。

5.2.2.1 角色和交易

区域医疗协同数据资料上传接收服务主要有两类角色参与，分别为区域医疗协同数据资料上传信息源和区域医疗协同数据资料上传接收服务组件，由区域医疗协同数据资料上传信息源向区域医疗协同数据资料上传接收服务组件发送申请，具体如图 5 所示。

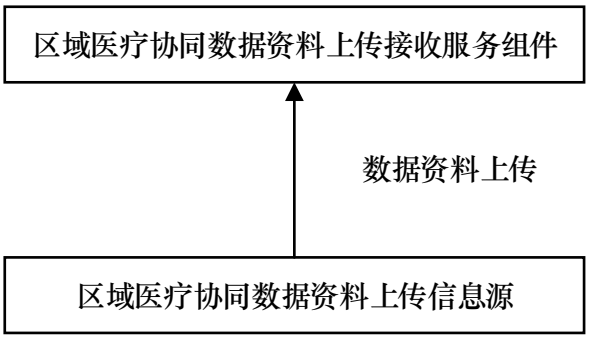

图 5 区域医疗协同数据资料上传接收服务角色交易图

5.2.2.2 角色交易选择

角色交易的选择，如表 2 所示。

表 2 区域医疗协同数据资料上传接收服务角色—交易关系表

角色	交易	选择
区域医疗协同数据资料上传信息源	上传数据资料	应有
区域医疗协同数据资料上传接收服务组件	上传数据资料	应有

5.2.2.3 交易流程

区域医疗协同数据资料上传接收服务的基本流程，如图 6 所示。

——区域医疗协同数据资料上传信息源发送区域医疗协同数据资料信息到区域医疗协同数据资料接收服务组件；

——区域医疗协同数据资料上传接收服务组件接收区域医疗协同数据资料后校验数据并存储。

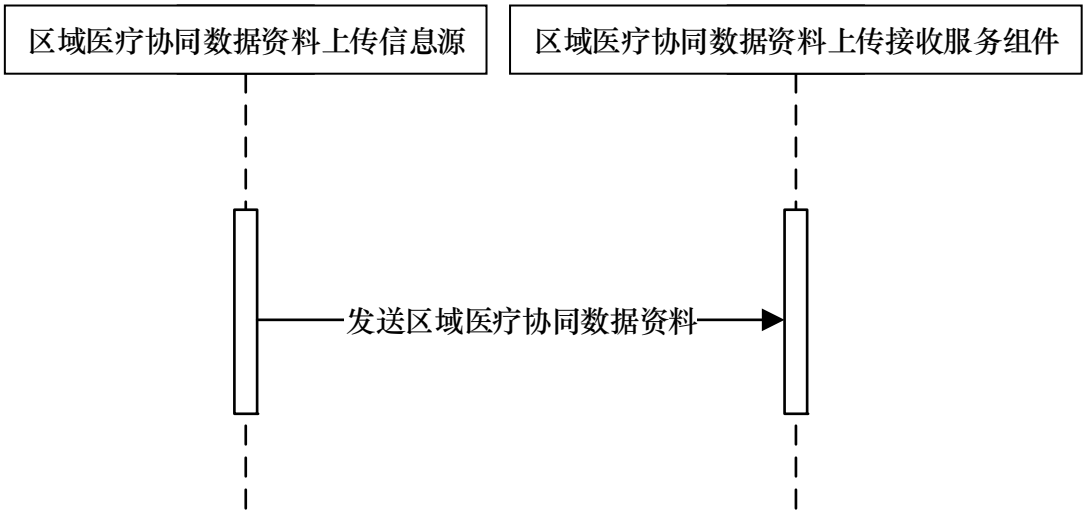

图 6 区域医疗协同数据资料上传接收服务时序图

5.2.3 区域医疗协同数据质量核查服务

区域医疗协同数据质量核查服务主要用于上传到区域医疗协同协同业务平台的数据资料进行质量核查。基本功能要求包括：

——具备区域医疗协同数据质量核查申请接收功能；

——具备区域医疗协同数据质量核查功能；

——具备区域医疗协同数据质量核查结果反馈功能。

5.2.3.1 角色和交易

区域医疗协同数据质量核查服务主要有两类角色参与，分别为区域医疗协同数据质量核查使用者和区域医疗协同数据质量核查服务组件，由区域医疗协同数据质量核查使用者向区域医疗协同数据质量核查服务组件发送核查信息，具体如图 7 所示。

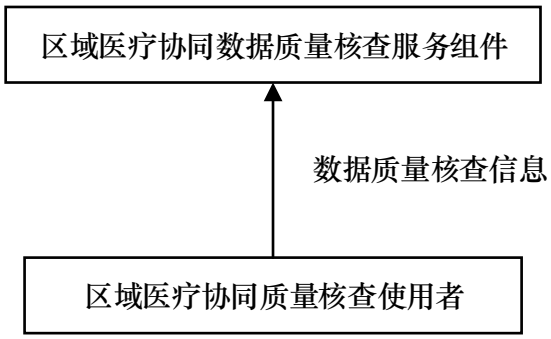

图 7 区域医疗协同数据质量核查服务角色交易图

5.2.3.2 角色交易选择

角色交易的选择，如表 3 **错误!未找到引用源。**所示。

表 3 区域医疗协同数据质量核查服务角色—交易关系表

角色	交易	选择
区域医疗协同数据质量核查使用者	数据质量核查	应有
区域医疗协同数据质量核查服务组件	数据质量核查	应有

5.2.3.3 交易流程

区域医疗协同数据质量核查服务的基本流程，如图 8 **错误!未找到引用源。**所示。

——区域医疗协同数据质量核查使用者发送数据质量核查信息到区域医疗协同数据质量核查服务组件；

——区域医疗协同数据质量核查服务组件接收区域医疗协同数据质量核查后，开始核查数据，并把核查结果返回给区域医疗协同数据质量核查使用者。

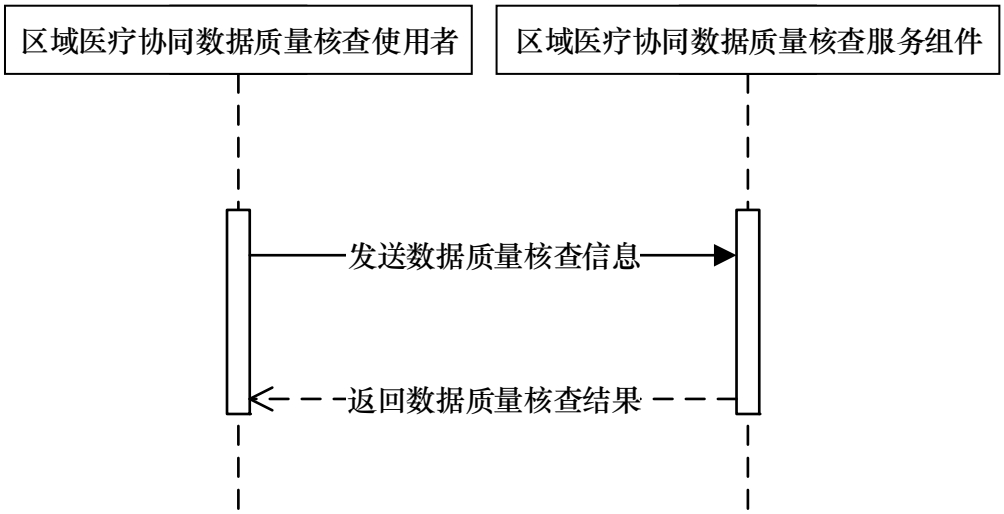

图 8 区域医疗协同数据质量核查服务时序图

5.2.4 区域医疗协同数据资料上传查询服务

区域医疗协同数据资料上传查询服务用于为各区域医疗协同应用提供数据资料的查询，如远程医疗数据资料、双向转诊数据资料、区域医学检验数据资料等上传结果查询，基本功能要求包括：

——具备区域医疗协同数据资料上传查询申请接收功能；

——具备区域医疗协同数据资料上传查询结果反馈功能。

5.2.4.1 角色和交易

区域医疗协同数据资料上传查询主要有两类角色参与，分别为区域医疗协同数据资料上传查询使用者和区域医疗协同数据资料上传查询服务组件，由区域医疗协同数据资料上传查询使用者向区域医疗协同数据资料上传查询服务组件发送查询信息，区域医疗协同数据资料上传查询服务组件接收查询信息并返回查询结果，具体如图 9 所示。

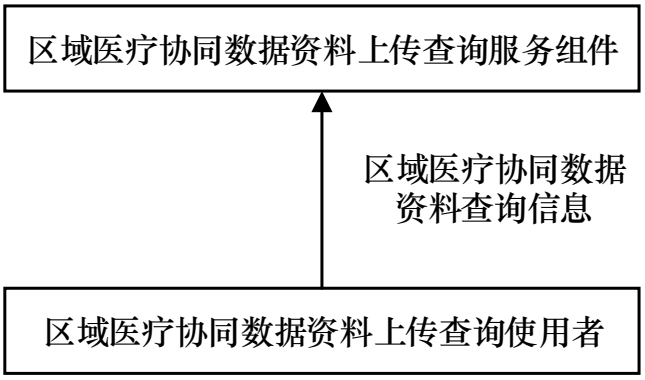

图 9 区域医疗协同数据资料上传查询服务角色交易图

5.2.4.2 角色交易选择

角色交易的选择，如表 4 所示。

表 4 区域医疗协同数据资料上传查询服务角色—交易关系表

角色	交易	选择
区域医疗协同数据资料上传查询使用者	上传数据资料	应有
区域医疗协同数据资料上传接收服务组件	上传数据资料	应有

5.2.4.3 交易流程

区域医疗协同数据资料上传查询服务的基本流程，如图 10 所示。

——区域医疗协同数据资料上传查询使用者发送区域医疗协同数据资料查询信息到区域医疗协同数据资料上传查询服务组件；

——区域医疗协同数据资料上传查询服务组件接收到请求后，判断是否有请求的申请信息，并把区域医疗协同数据资料信息返回给区域医疗协同数据资料查询使用者。

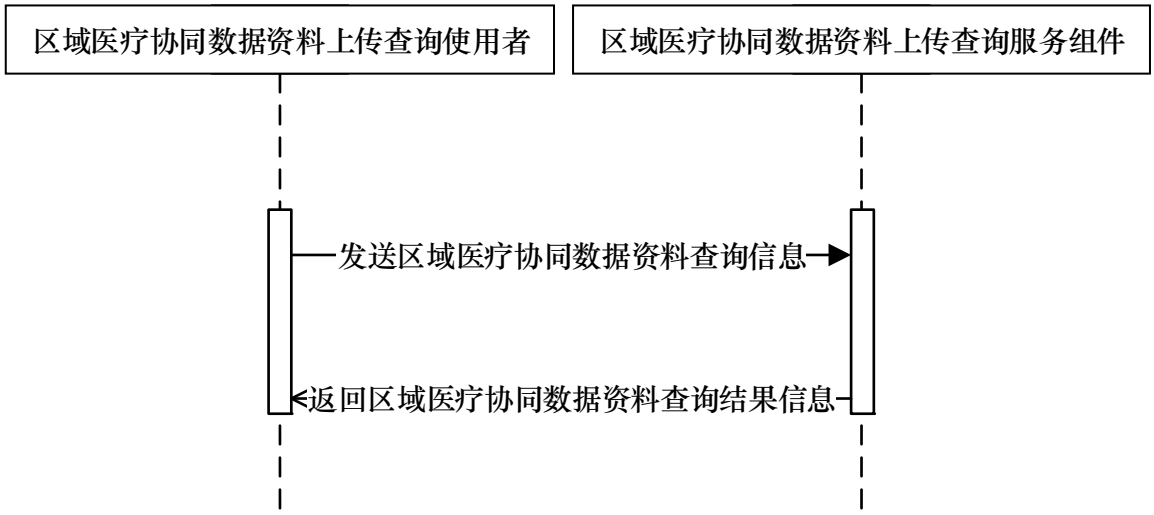

图 10 区域医疗协同数据资料上传查询服务时序图

5.2.5 区域医疗协同申请信息查询服务

区域医疗协同申请信息查询服务用于区域医疗协同申请信息查询的接收与查询结果的反馈，如远程医疗申请信息查询、双向转诊申请信息查询、区域医学检验申请信息查询等查询，基本功能要求包括：

——具备区域医疗协同申请信息查询接收功能；

——具备区域医疗协同申请信息查询结果反馈功能。

5.2.5.1 角色和交易

区域医疗协同申请信息查询服务角色主要有两类组成，分别为区域医疗协同申请信息查询使用者和区域医疗协同申请信息查询服务组件，由区域医疗协同申请信息查询使用者向区域医疗协同申请信息查询服务组件发送查询申请信息请求，区域医疗协同申请信息查询服务组件返回查询结果。如图 11 所示。

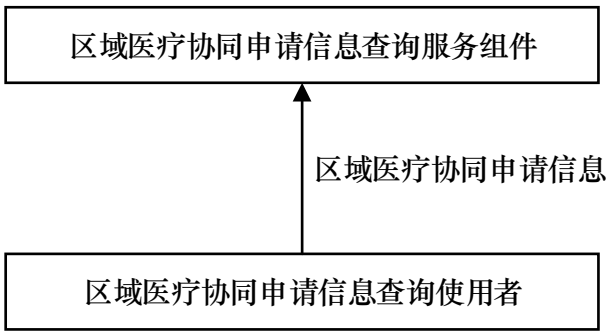

图 11 区域医疗协同申请信息查询服务角色交易图

5.2.5.2 角色交易选择

角色交易的选择，如表 5 所示。

表 5 区域医疗协同申请信息查询服务角色—交易关系表

角色	交易	选择
区域医疗协同申请信息查询使用者	查询申请信息	应有
区域医疗协同申请信息查询服务组件	查询申请信息	应有

5.2.5.3 交易流程

区域医疗协同申请信息查询基本流程，如图 12 所示。

——区域医疗协同申请信息查询使用者向区域医疗协同申请信息查询服务组件发送查询申请信息请求；

——区域医疗协同申请信息查询服务组件接收到请求后，判断是否有请求的申请信息，并把申请信息返回给区域医疗协同申请信息查询使用者。

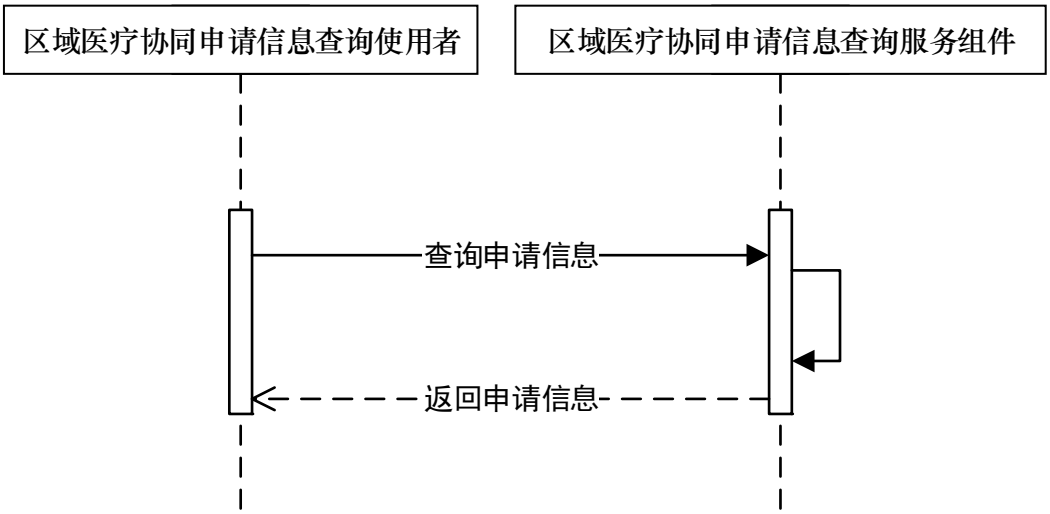

图 12 区域医疗协同申请信息查询服务时序图

5.3 区域医疗协同数据资料管理服务

区域医疗协同数据资料的管理服务是指对区域医疗协同的数据资料档案进行管理,包括建档、注销、变更等。服务包括区域医疗协同文档注册服务、区域医疗协同事件注册服务、区域医疗协同索引服务。

5.3.1 区域医疗协同文档注册服务

区域医疗协同文档注册服务，可以根据文档的内容维护每个注册文档的元数据，包括在文档库中的存储路径，可根据用户的查询条件返回文档或文档集。

5.3.2 区域医疗协同事件注册服务

为实现区域医疗协同各应用系统对数据资料信息的共享和交换，需要以区域医疗协同患者为单位，

对患者获得的医疗卫生服务活动的事件信息进行注册。

事件注册就是建立一个事件目录，目录中的每个条目由描述该事件的关键信息构成，在注册时，需要注册从区域医疗协同的文档中提取的与事件相关的元数据，注册的同时，事件信息将被作为患者与文档之间的关联关系，便于使用者可以通过事件的途径获取相关的文档。

5.3.3 区域医疗协同索引服务

区域医疗协同各应用系统用户在被授权的情况下，可以通过索引服务查看患者的区域医疗协同数据资料，以及相关的文档目录和摘要信息。再结合区域医疗协同数据资料存储服务可以实现文档信息的即时展示，使用户全面的了解患者的诊疗信息。

区域医疗协同索引服务全面掌握区域医疗协同各应用系统所有关于患者的诊疗信息事件，包括患者的就诊时间、科室、接收的医疗服务、医疗记录。通过区域医疗协同索引服务可以查看患者的诊疗事件信息，以及事件信息所涉及的文档目录和摘要信息。基本功能包括：

——具备静态文档注册功能；

——具备查询相关医疗静态文档索引的功能。

5.4 区域医疗协同数据资料存储服务

区域医疗协同资料存储服务是以标准化的方式存储区域医疗协同资料数据，为区域医疗协同资料的共享和管理，并为相关协同服务提供支持。根据区域医疗协同资料数据的分类，区域医疗协同资料存储服务可分为六类：个人基本信息资料存储、电子病历信息资料存储、健康档案信息资料存储、会诊信息资料存储、影像数据资料存储、教学资源资料存储。用于接收电子病历文档、影像、视频资料，并将文档注册到索引服务中，同时对文档的版本及生命周期管理，它还提供文档接收服务。基本功能要求包括：

——具备接收区域医疗协同资料数据功能；

——具备向索引库注册区域医疗协同资料数据功能；

——具备向使用者提供区域医疗协同资料数据功能。

区域医疗协同资料存储服务基于 XDS 规范包括文档库、文档注册、文档源和文档使用者等角色，如图 13、表 6 所示。

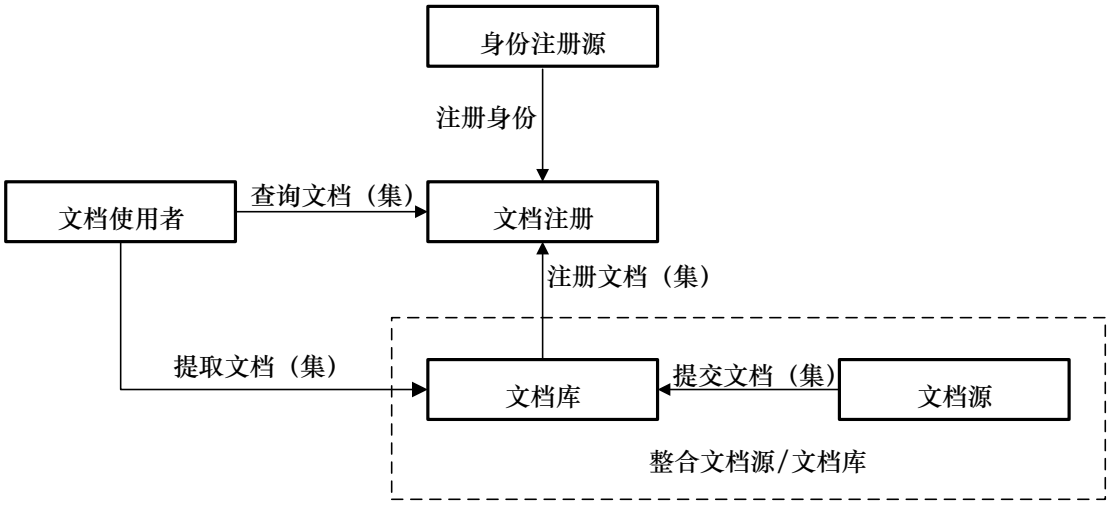

图 13 区域医疗协同资料存储服务角色交易图

表 6 区域医疗协同资料存储角色和交易关系表

角色	交易	选择
身份注册源	注册身份	可选
文档注册	注册文档（集）	应有
	查询文档（集）	应有
	提取文档（集）	可选
文档库	提供文档（集）	应有
	注册文档（集）	应有
	提取文档（集）	应有
文档使用者	查询文档（集）	应有
	提取文档（集）	应有
文档源	提供文档（集）	应有
整合文档源/文档库	注册文档（集）	应有

5.4.1 角色

5.4.1.1 文档源

文档源是文档的提交者，由它将文档提交给文档库。文档源所提交的文档（集）需要满足文档库能把文档信息注册到文档注册角色中的要求。

5.4.1.2 文档使用者

文档使用者为一个向文档注册角色提交一组指定查询条件的，并由文档库向其返回一个或多个符合条件的文档（集）的角色。

5.4.1.3 文档注册

文档注册角色根据文档条目中的内容维护每一个注册文档的元数据，并包括在文档库中存储联机地址，供文档使用者在查询文档时使用。文档注册角色需要根据文档使用者的特定查询条件返回文档（集）目录。文档注册角色也可提供对文档使用者和文档源的身份认证。

5.4.1.4 文档库

文档库是文档注册的持久化的储存空间，也要提供相关文档注册角色的注册消息，并为给文档注册角色供文档使用者提取文档分配一个访问地址。

5.4.1.5 身份注册源

身份注册源为个人提供唯一身份标识，并且维护个人的标识特征，身份注册源在进行文档交互过程中提供个人标识的有效性给文档注册角色。

5.4.1.6 整合文档源/文档库

整合文档源/文档库是将文档源和文档库两个角色的功能整合，能同时直接对外提供文档注册和提取文档服务。

5.4.2 交易

5.4.2.1 提交文档（集）

提交文档（集）为文档源角色向文档库角色发起的提供和注册文档的交易。对提交的集合中的文档，文档源角色既把文档作为一个不透明的字节流来提供，又向文档库提供相应的文档元数据文档的存储库负责永久存储这些文件，并使用文档注册交易，将从文档源角色获取的文档信息对文档进行注册。

5.4.2.2 注册文档（集）

注册文档（集）为文档库角色发起的注册文档集交易。这一交易允许文档库角色通过提供每个文档要注册的元数据来使用文档注册角色来注册一个或多个文档。这个文档元数据将被用来在注册时生成一个 XDS 文档条目。在允许文档注册前，文档注册角色要保证文档元数据的正确性。若文档集中的一个或多个文档元数据校验未通过，则本次所有文档注册失败。为支持复合文档，一个 XDS 文档可能是一个多部分文档。文档库应把多部分文档作为一个不透明实体来处理根据 XDS 规范，文档库不必分析或处理多

部分文档的多部分机构和每部分内容。

5.4.2.3 查询文档（集）

查询文档（集）交易由文档使用者角色向文档注册角色发起。文档注册角色按照文档使用者角色指定的查询条件搜索本地文档库，并返回一组符合指定条件的元数据的文档列表，其中的元数据包括在一个或多个文档库，其中还包括每个相应文档的位置和标识符。

5.4.2.4 提取文档（集）

提取文档（集）为文档使用者角色向文档库发起的提取文档交易。文档库将根据文档注册索引信息返回文档使用者指定的文档。为支持复合文档，XDS 文档可以是一个多部分文档。文档使用者应采取适当的方法使用户能够获取多部分文档的内容。

5.4.2.5 注册身份

注册身份交易由身份注册源向文档注册角色发起的身份标识注册的交易。它发送个人标识和相关的人口学数据，如身份证件号码、姓名等，这些标识信息是在建立个人身份或者关键人口数据被修改或合并时被获取的。在 XDS 集成模式中是为了把已经在相关域中注册的个人标识信息发送给注册者。

5.4.3 文档处理

5.4.3.1 概述

文档处理角色交易的选择，如表 7 所示。

表 7 文档处理角色和交易关系表

角色	交易	选择
文档源	文档替换	应有
	文档新增	应有
	文档变更	应有
	文件夹管理	应有
整合文档源/文档库	文档替换	应有
	文档新增	应有
	文档变更	应有
	文件夹管理	应有

5.4.3.2 文档替换

文档源、整合文档源/文档库两个角色应当提供这样的功能，将已存在文档库中的一份文档替换为当前有提交的文档，同时分组文档用户可以提交用于替换的最新元数据及其数据元 ID。

5.4.3.3 文档新增

文档源、整合文档源/文档库两个角色应当提供这样的功能，提交一份文档用于建立新文档或补充已存在文档库中的另一份文档。

5.4.3.4 文档变更

文档源、整合文档源/文档库两个角色应当提供这样的功能，提交一份文档转换已存在在文档库中的另一个文档。

5.4.3.5 文件夹管理

文档源应该提供以下操作功能：

——创建新文件夹；

——添加一个或多个文档到一个文件夹中。

5.5 区域医疗协同数据资料调阅服务

区域医疗协同数据资料调阅服务用于处理区域医疗协同业务应用子平台内与数据定位和管理相关的复杂任务。该服务包括相关的数据访问服务、组装服务以及标准化服务。区域医疗协同数据资料调阅服务负责分析来自外部资源的请求，响应外部子系统的检索、汇聚和返回数据。

5.5.1 数据访问服务

5.5.1.1 调阅展示服务

5.5.1.1.1 角色和交易

交易流程，如图 14 所示。

——区域医疗协同数据资料调阅使用者发起获取专有展示文档和获取调阅展示文档交易；

——区域医疗协同数据资料调阅服务组件接收获取专有展示文档和获取调阅展示文档交易的请求。

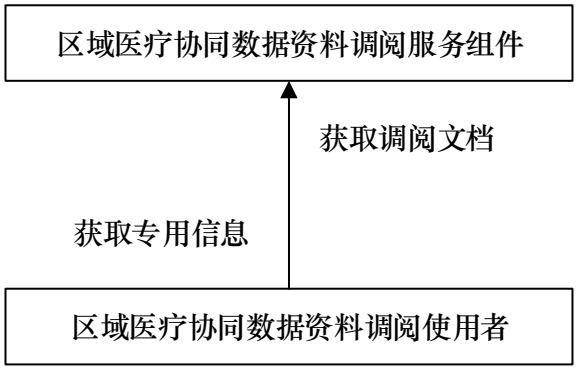

图 14 调阅展示角色交易图

5.5.1.1.2 角色交易选择

角色交易的选择，如表 8所示。

表 8 调阅展示角色

角色	交易	选择
区域医疗协同数据资料调阅服务组件	获取专有信息	可选
	获取展示文档	应有
区域医疗协同数据资料调阅使用者	获取专有信息	可选
	获取展示文档	应有

5.5.1.1.3 交易流程

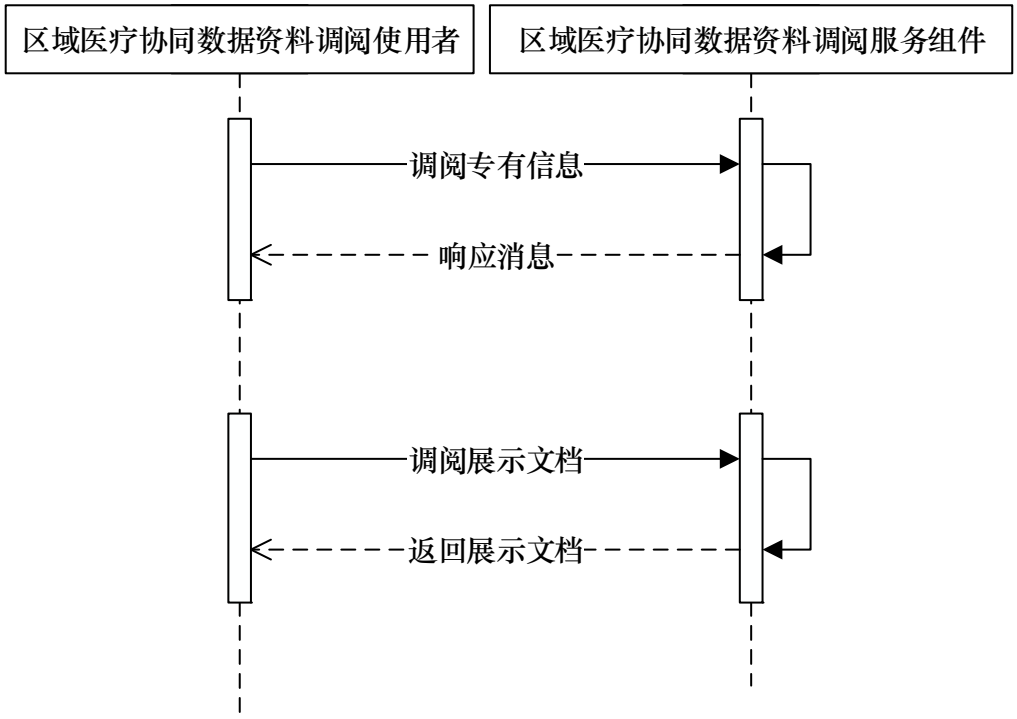

图 15 调阅展示服务时序图

区域医疗协同数据资料调阅展示服务的基本流程，如图 15 所示：

——区域医疗协同数据资料调阅使用者向区域医疗协同数据资料调阅展示服务提交请求消息，区域医疗协同数据资料调阅展示服务向个人注册服务组件请求个人 ID；

——区域医疗协同数据资料调阅展示服务根据个人 ID 向档案服务发起查询索引交易，返回索引信息；然后根据索引信息向区域医疗协同数据资料调阅展示服务组件发起展示调阅文档交易，查询成功返回调阅文档；

——区域医疗协同数据资料调阅展示服务查询失败返回异常响应消息。

5.5.1.2 调阅目录服务

5.5.1.2.1 角色和交易

区域医疗协同数据资料调阅使用者请求调阅目录服务，区域医疗协同数据资料调阅服务组件接收调阅请求，并返回结构化数据，如图 16 所示。

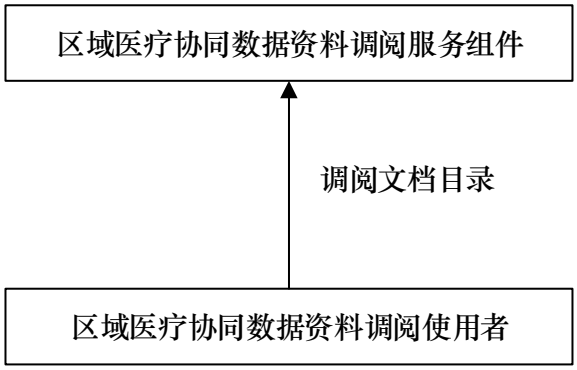

图 16 区域医疗协同数据资料调阅目录角色交易图

5.5.1.2.2 角色交易选择

角色交易的选择，如表 9所示。

表 9 区域医疗协同数据资料调阅目录角色

角色	交易	选择
区域医疗协同数据资料调阅服务组件	调阅目录服务	应有
区域医疗协同数据资料调阅使用者	调阅目录服务反馈	应有

5.5.1.2.3 交易流程

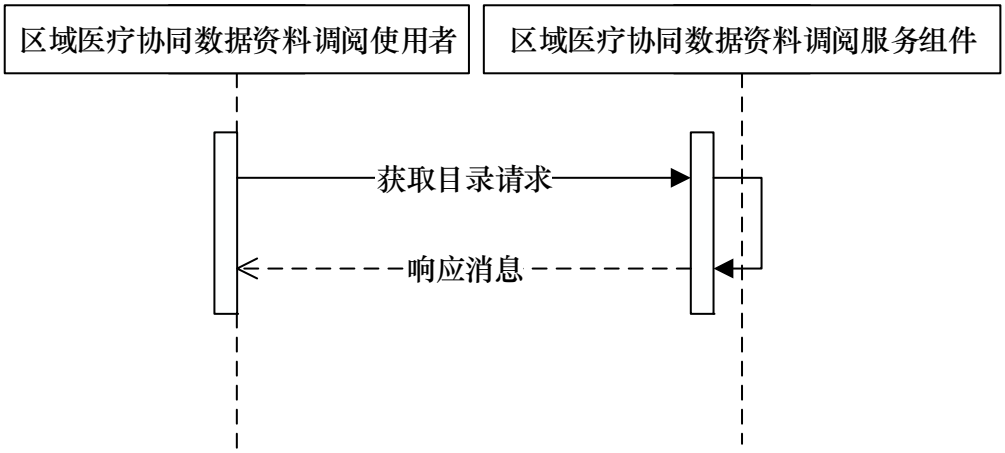

图 17 区域医疗协同数据资料调阅目录时序图

区域医疗协同数据资料调阅目录服务的基本流程，如图 17 所示：

——区域医疗协同数据资料调阅使用者向区域医疗协同数据资料调阅服务提交请求消息，其请求应包括个人标识信息；

——区域医疗协同数据资料调阅服务根据个人标识信息查询，查询成功返回按时间排序的结构化数

据；

——区域医疗协同数据资料调阅服务查询失败时返回异常响应消息。

5.5.2 组装服务

调用不同的组件生成多个结果集。组装服务将把这些结果集组合成一定输出格式。这些服务可使用组合模板的方式来实现这些功能：

——个人基本信息组装服务：基于个人注册服务提取个人基本信息。

——区域医疗协同数据资料目录组装服务：按照多种维度和多层级来形成区域医疗协同数据资料目录。如：患者诊疗记录信息以时间轴方式展示。

5.5.3 标准化服务

标准化服务是在平台互联互通性执行的语境中被调用以转换成不同形式下描述的数据。这个服务常用于应用标准，把特定的输入串转化成符合标准化基础的编码串。数据的格式和实质含义都可以转换。特殊的逻辑和编码表常用于完成这种转化。标准化主要是代码转换服务和数据结构的标准化。可以基于术语和字典注册服务开发。该服务基本功能包括：

——具备标准化编码转换功能；

——具备数据标准格式转换功能；

——具备标准化数据输出功能。

5.6 区域医疗协同结果信息反馈服务

区域医疗协同结果信息反馈服务用于处理区域医疗协同业务应用子平台内与区域医疗协同结果数据的接收、处理、储存及查询相关的任务。该服务包含区域医疗协同结果信息接收服务、区域医疗协同结果信息订阅服务、区域医疗协同结果信息发布服务和区域医疗协同结果信息查询服务。

5.6.1 区域医疗协同结果信息接收服务

区域医疗协同结果信息接收服务用于接收区域医疗协同结果信息源产生的区域医疗协同结果信息数据，对所接收的结果数据进行标准化校验，并将最终校验通过的合法数据进行存储处理。基本功能要求包括：

——具备区域医疗协同结果信息数据接收功能；

——具备区域医疗协同结果信息数据标准化校验功能；

——具备区域医疗协同结果信息数据储存功能。

5.6.1.1 角色和交易

区域医疗协同结果信息接收服务角色主要有两类，分别为区域医疗协同结果信息源和区域医疗协同结果信息接收服务组件，由区域医疗协同结果信息源向区域医疗协同结果信息接收服务组件发送结果信息，区域医疗协同结果信息接收服务组件接收结果信息并存储。如图 18 所示。

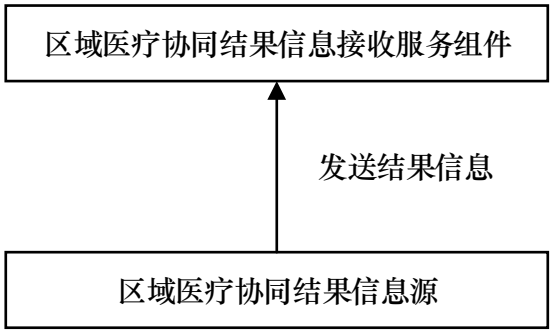

图 18 区域医疗协同结果信息接收服务角色交易图

5.6.1.2 角色交易选择

角色交易的选择，如表 10 所示。

表 10 区域医疗协同结果信息接收服务角色—交易关系表

角色	交易	选择
区域医疗协同结果信息源	接收结果信息	应有
区域医疗协同结果信息接收服务组件	接收结果信息	应有

5.6.1.3 交易流程

区域医疗协同结果信息接收服务基本流程，如图 19 所示。

——区域医疗协同结果信息源将结果信息发送到区域医疗协同结果信息接收服务组件；

——区域医疗协同结果信息接收服务组件接收校验数据并存储。

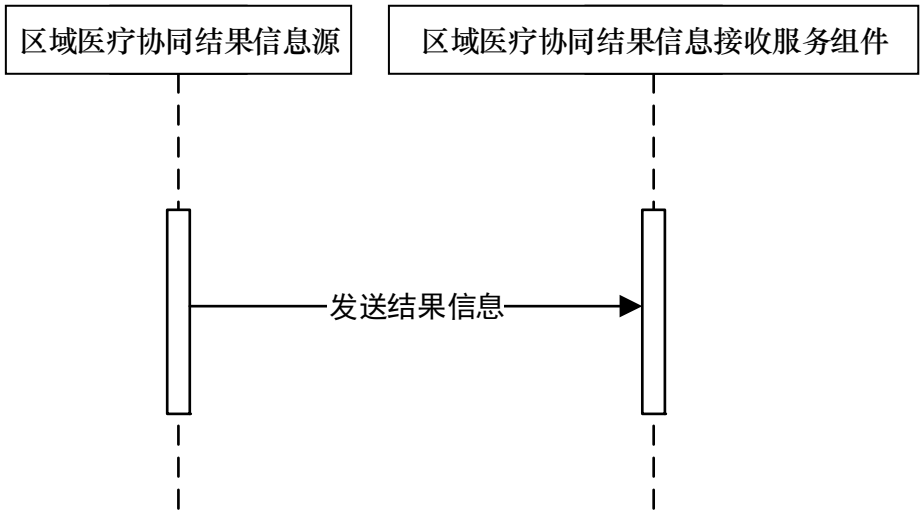

图 19 区域医疗协同结果信息接收服务时序图

5.6.2 区域医疗协同结果信息订阅服务

区域医疗协同结果信息订阅服务用于区域医疗协同结果信息使用者向区域医疗协同结果信息订阅服务组件发送订阅请求，区域医疗协同结果信息订阅服务组件接收请求信息并储存。基本功能要求包括：

——具备区域医疗协同结果信息订阅请求接收功能；

——具备区域医疗协同结果信息订阅者身份验证功能；

——具备区域医疗协同结果信息订阅请求合理性验证功能；

——具备区域医疗协同结果信息订阅请求信息储存功能。

5.6.2.1 角色和交易

区域医疗协同结果信息订阅服务角色主要有两类，分别为区域医疗协同结果信息使用者和区域医疗协同结果信息订阅服务组件，由区域医疗协同结果信息使用者向区域医疗协同结果信息订阅服务组件发送订阅请求，区域医疗协同结果信息订阅服务组件接收并存储。如图 20 所示。

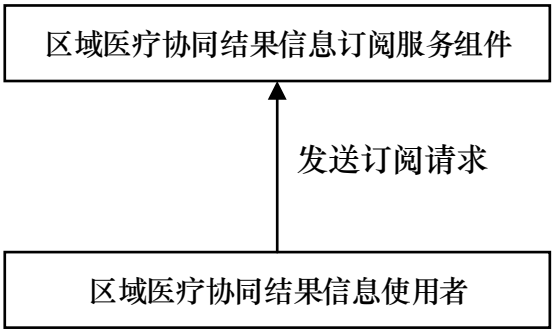

图 20 区域医疗协同结果信息订阅服务角色交易图

5.6.2.2 角色交易选择

角色交易的选择，如表 11 所示。

表 11 区域医疗协同结果信息订阅服务角色—交易关系表

角色	交易	选择
区域医疗协同结果信息使用者	订阅结果信息	应有
区域医疗协同结果信息订阅服务组件	订阅结果信息	应有

5.6.2.3 交易流程

区域医疗协同结果信息订阅服务基本流程，如图 21 所示。

——区域医疗协同结果信息使用者将订阅结果信息发送到区域医疗协同结果信息订阅服务组件；

——区域医疗协同结果信息订阅服务组件接收校验数据并存储。

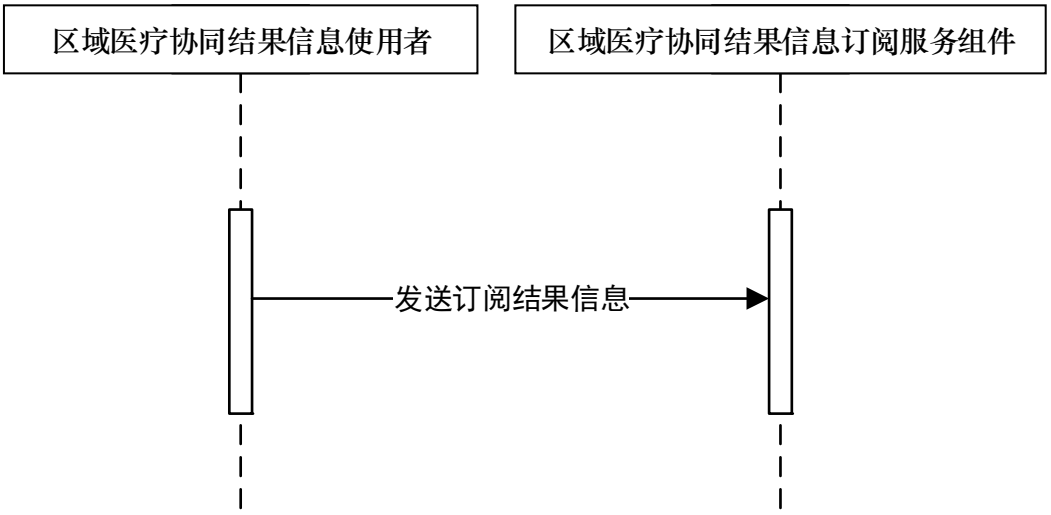

图 21 区域医疗协同结果信息订阅服务时序图

5.6.3 区域医疗协同结果信息发布服务

区域医疗协同结果信息发布服务用于区域医疗协同结果信息发布服务组件向区域医疗协同结果信息订阅者发布区域医疗协同结果信息，区域医疗协同结果信息订阅者接收结果信息。基本功能要求包括：

——具备区域医疗协同结果信息发布功能；

——具备区域医疗协同结果信息接收功能。

5.6.3.1 角色和交易

区域医疗协同结果信息发布服务角色主要有区域医疗协同结果信息订阅者和区域医疗协同结果信息发布服务组件两类，由区域医疗协同结果信息发布服务组件向区域医疗协同结果信息订阅发布查询区

域医疗协同结果信息请求，区域医疗协同结果信息发布服务组件发布结果。如图 22 所示。

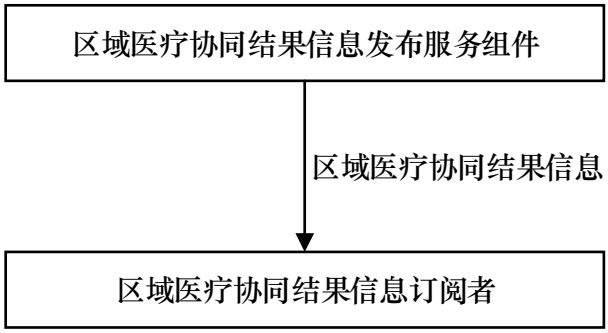

图 22 区域医疗协同结果信息发布服务角色交易图

5.6.3.2 角色交易选择

角色交易的选择，如表 12 所示。

表 12 区域医疗协同结果信息发布服务角色

角色	交易	选择
区域医疗协同结果信息订阅者	发布结果信息	应有
区域医疗协同结果信息发布服务组件	发布结果信息	应有

5.6.3.3 交易流程

区域医疗协同结果信息发布服务基本流程，如图 23 所示。

——区域医疗协同结果信息发布服务组件将结果信息发布给区域医疗协同结果信息订阅者；

——区域医疗协同结果信息订阅者接收结果信息。

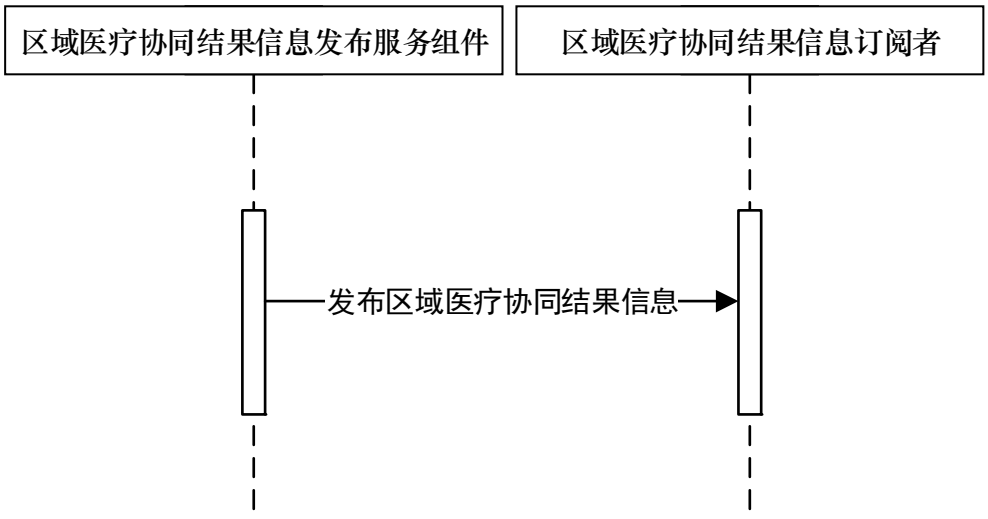

图 23 区域医疗协同结果信息发布服务时序图

5.6.4 区域医疗协同结果信息查询服务

区域医疗协同结果信息查询服务用于区域医疗协同结果信息查询使用者向区域医疗协同结果信息查询服务组件发送区域医疗协同结果信息查询请求，区域医疗协同结果信息查询服务组件向区域医疗协同结果信息查询使用者返回区域医疗协同结果信息。基本功能要求包括：

——具备区域医疗协同结果信息查询请求功能；

——具备区域医疗协同结果信息查询请求验证功能；

——具备区域医疗协同结果信息查询结果回传功能。

5.6.4.1 角色和交易

区域医疗协同结果信息查询服务角色主要有两类角色，分别为区域医疗协同结果信息查询使用者和区域医疗协同结果信息查询服务组件，由区域医疗协同结果信息查询使用者向区域医疗协同结果信息查询服务组件发送查询区域医疗协同结果信息请求，区域医疗协同结果信息查询服务组件返回查询结果。如图 24 所示。

#

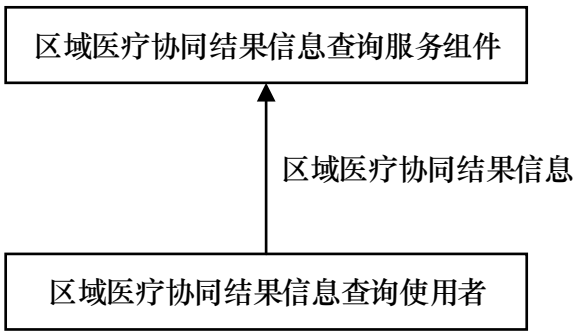

图 24 区域医疗协同结果信息查询服务角色交易图

5.6.4.2 角色交易选择

角色交易的选择，如表 13 所示。

表 13 区域医疗协同结果信息查询服务角色

角色	交易	选择
区域医疗协同结果信息查询使用者	查询结果信息	应有
区域医疗协同结果信息查询服务组件	查询结果信息	应有

5.6.4.3 交易流程

区域医疗协同结果信息查询基本流程，如图 25 所示。

——区域医疗协同结果信息查询使用者向区域医疗协同结果信息查询服务组件发送结果信息查询请求；

——区域医疗协同结果信息查询服务组件接收到请求后，判断是否有请求的结果信息，并把区域医疗协同结果信息返回给区域医疗协同结果信息查询使用者。

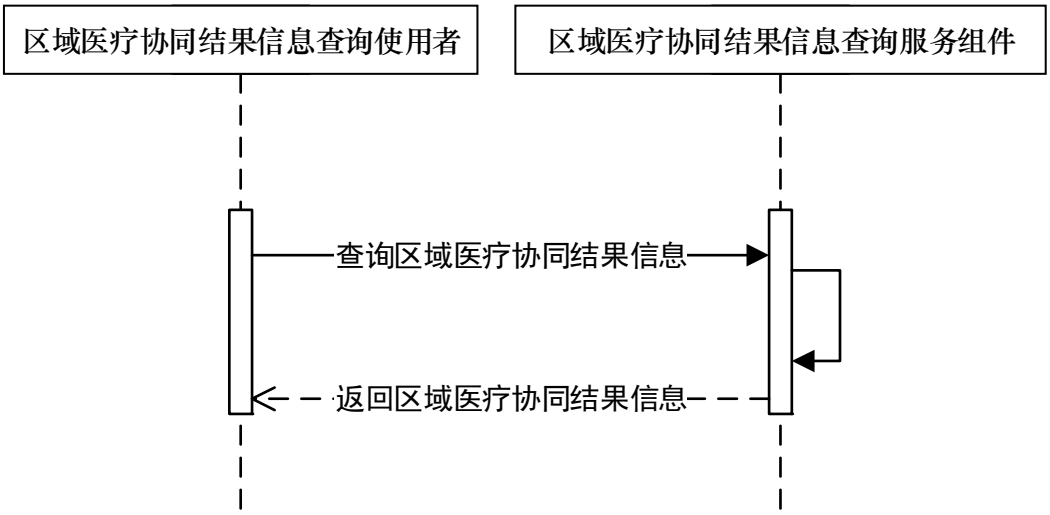

图 25 区域医疗协同结果信息查询服务时序图

5.7 区域医疗协同业务协同服务

区域医疗业务协同服务是用于医疗机构之间相互调用业务服务的整合服务。基本功能要求包括：

——具备协同服务请求接收功能；

——具备协同服务请求验证功能；

——具备业务服务调用功能；

——具备业务服务调用结果回传功能。

5.7.1 角色和交易

区域医疗业务协同服务包括三类角色，分别为：区域医疗业务协同服务组件、协同服务使用者和业务服务提供者。业务服务提供者以服务的形式把自己的功能和数据注册到区域医疗业务协同服务组件中，区域医疗业务协同服务组件对这些服务进行整合并对外发布一组协同服务；协同服务使用者根据业务需要调用协同服务；区域医疗业务协同服务组件根据协同服务使用者的请求，通过调用业务服务提供者提供的服务，并进行整合后响应协同服务使用的请求，如图 26 所示。

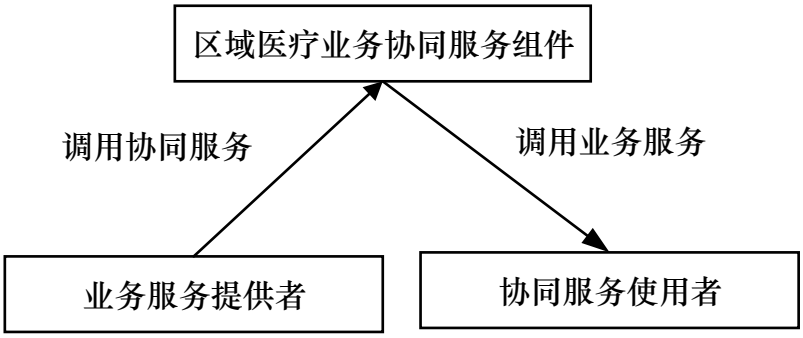

图 26 区域医疗业务协同服务角色交易图

5.7.2 角色交易选择

角色交易的选择，如表 14 所示。

表 14 区域医疗业务协同服务角色—交易关系表

角色	交易	选择
业务服务提供者	调用业务服务	应有
协同服务使用者	调用协同服务	应有
区域医疗业务协同服务组件	调用业务服务	应有
	调用协同服务	

5.7.3 交易流程

以远程双向转诊为例，基本交易流程包括：

——下级医院(作为协同服务使用者)调用区域医疗业务协同服务组件中的双向转诊资源查询服务；

——区域医疗业务协同服务组件调用上级协议医院（作为业务服务提供者）的转诊资源查询服务；

——上级协议医院的转诊资源查询服务返回转诊资源响应给区域医疗业务协同服务组件；

——区域医疗业务协同服务组件将收到的上级协议医院的转诊资源响应，返回给下级医院。

5.8 区域医疗协同业务应用子平台与区域卫生信息平台等其他平台的交互服务

5.8.1 与区域卫生信息平台的交互服务

5.8.1.1 基本要求

区域协同业务应用子平台与区域卫生信息平台互通互联应符合《WST 448-2014 基于居民健康档案的区域卫生信息平台技术规范》要求，交互规范应符合《WS XXX-20XX 区域卫生信息平台交互规范》要求，电子健康档案共享文档应符合《WS XXX-20XX 电子健康档案共享文档规范》规定的共享文档中包含

的数据信息，交互的数据要求符合《WS 363-2011 卫生信息数据元目录》、《WS 364-2011 卫生信息数据元值域代码》、《电子病历基本架构与数据标准（试行）》等标准的要求。

5.8.1.2 注册服务调用

基本功能要求包括：

——具备调用区域卫生信息平台的个人信息注册服务的功能；

——具备调用区域卫生信息平台的医务卫生人员注册服务的功能；

——具备调用区域卫生信息平台的卫生机构（科室）注册服务的功能；

——具备调用区域卫生信息平台的术语和字典注册的功能。

5.8.1.3 健康档案调阅服务调阅

基本功能要求包括：

——具备调用区域卫生信息平台的调阅预判服务功能；

——具备调用区域卫生信息平台的调阅展示服务功能；

——具备调用区域卫生信息平台的调阅目录服务功能；

——具备调用区域卫生信息平台的调阅摘要服务功能。

——交互规范应符合区域卫生信息平台交互规范。

5.8.1.4 病历数据调阅服务调用

基本功能要求包括：

——具备调用区域卫生信息平台的病历数据查询服务功能；

——病历数据的范围应符合 WS/T 448-2014 中的 10.3.1。

5.8.2 与医院信息平台的交互服务

5.8.2.1 基本要求

区域协同业务应用子平台与医院信息平台互通互联应符合《WST 447-2014 基于电子病历的医院信息平台技术规范》要求，交互规范应符合《WS XXX-20XX 医院信息平台交互规范》要求，电子病历共享文档应符合《WS XXXX-XXXX 电子病历共享文档规范》规定的共享文档中包含的数据信息，交互的数据要求符合《WS 363-2011 卫生信息数据元目录》、《WS 364-2011 卫生信息数据元值域代码》、《电子病历基本架构与数据标准（试行）》等标准的要求。

5.8.2.2 注册服务调用

基本功能要求包括：

——具备调用医院信息平台的个人信息注册服务的功能；

——具备调用医院信息平台的医务卫生人员注册服务的功能；

——具备调用医院信息平台的卫生机构（科室）注册服务的功能；

——具备调用医院信息平台的术语和字典注册的功能。

5.8.2.3 区域医疗协同门诊就诊登记接收服务调用

区域医疗协同门诊就诊登记接收服务调用应具备调用医院信息平台门诊就诊查询服务功能。

5.8.2.4 区域医疗协同住院就诊登记接收服务调用

区域医疗协同住院就诊登记接收服务调用应具备调用医院信息平台住院就诊查询服务功能。

5.8.2.5 区域医疗协同病历数据检索接收服务调用

区域医疗协同病历数据检索接收服务调用应具备调用医院信息平台病历数据检索服务功能。

5.8.2.6 区域医疗协同病历数据查询接收服务调用

区域医疗协同病历数据查询接收服务调用应具备调用医院信息平台病历数据查询服务功能。

5.9 信息安全及隐私服务

信息安全及隐私服务包括用户管理和权限管理、信息安全服务、隐私保护服务、审计追踪服务等。

5.9.1 用户管理和权限管理

5.9.1.1 用户管理

——应确保访问区域医疗协同应用子平台的所有实体（用户和系统）采用唯一身份标识，并对实体身份进行统一管理，包括：

- 对区域医疗协同应用子平台各类实体信息进行数字身份的定义和标识；
- 实现数字身份流程化管理，控制数字身份的整个生命周期，支持身份信息申请、审批、变更及撤销等管理操作；
- 集中管理用户身份属性信息（包括姓名、性别、出生日期、民族、婚姻状况、职业、工作单位、住址、有效身份证件号码、联系电话等）；
- 确保每个用户应具有唯一的身份标识和唯一的身份鉴别信息；
- 如果进行用户和系统之间的相互身份鉴别，则系统也应具有唯一的身份鉴别信息；

- 确保用户和系统的身份鉴别信息应是不可伪造；
- 提供用户自助服务功能（例如身份注册申请、修改、密码重置等）。

——应根据用户对区域医疗协同应用子平台系统的使用性质的不同进行用户分类管理，包括：

- 将用户分为业务用户和管理用户两大类，根据用户职责对用户分类进行细化；
- 创建用户角色和工作组，按照一定规则将具有相同属性或特征的用户划分为一组，进行用户组管理。

5.9.1.2 权限管理

——系统支持对用户、角色、资源和权限的标准化管理，实施权限管理和权限的分配，包括：

- 应支持基于“用户一角色/用户组一应用资源”的授权模型，制定授权策略；
- 确保每个授权用户应具有唯一的用户标识（ID）和唯一的身份鉴别信息；
- 提供用户角色创建服务：创建用户角色和工作组，为各使用者分配独立用户名的功能；
- 为各角色、工作组和用户进行授权并分配相应权限，提供取消用户的功能，用户取消后保留该用户在系统中的历史信息；
- 创建、修改患者病历访问规则，根据业务规则对用户自动临时授权的功能（如限定访问时间或访问资料范围等），满足患者病历灵活访问授权的需要；
- 提供增加、修改、删除和查询用户权限的功能；
- 应支持分层次授权，避免集中授权复杂性，提高授权的准确性；
- 业务权限和管理权限严格分开，业务用户不应具备管理权限；
- 应对所有的授权行为进行审计跟踪，提供记录权限修改操作日志的功能。

5.9.2 信息安全

5.9.2.1 身份认证

——应提供专用的认证模块对访问平台系统的用户和系统进行身份鉴别，并对鉴别数据进行保密性和完整性保护，应选择以下身份认证机制中的两种或两种以上组合进行身份认证，包括：

- 基于PKI/CA体系的数字证书认证方式：数字证书需存储于硬件证书载体USBKey并进行PIN口令保护、私钥和PIN码应在USBKey内生成；

- 用户名/口令认证方式：口令设置应具备一定的复杂度、口令设置定期更换要求、口令字符输人时应不显示原始字符、口令信息在传输及存储过程中需采用密码技术加密保护、管理员有权限重置密码；
- 基于人体生物特征识别的认证方式；
- 其他具有相应安全强度的认证方式。

——应支持登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施，包括：

- 设置账户锁定阈值时间，当失败的用户身份鉴别尝试次数达到规定的数值时，应能够终止用户与系统之间的会话；
- 用户多次登录错误时，自动锁定该账户，管理员有权限解除账户锁定；
- 应对身份鉴别失败事件进行审计跟踪。

——应支持单点登录系统功能，用户只经过一次身份认证即可访问不同的业务系统；

——应提供节点认证服务。各个接入总线的服务进行双向身份认证，保证服务提供方可靠。

5.9.2.2 访问控制

应启用访问控制功能，应在安全策略控制范围内，据安全策略控制用户对文件、数据库表等客体的访问，访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作。技术要求包括：

——访问控制主体的粒度为用户级,客体的粒度为文件或数据库表级;访问操作包括对客体的创建、读、写、修改和删除等；

——基于授权策略建立自主访问控制列表；

——应按用户和系统之间的允许访问规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户；

——应依据安全策略严格控制用户对有敏感标记重要信息资源的操作；

——应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为服务级；

——应在会话处于非活跃一定时间或会话结束后终止连接；

——应能够对应用系统的最大并发会话连接数进行限制；

——应能够对单个账户的多重并发会话进行限制；

——应能够对一个时间段内可能的并发会话连接数进行限制；

——应能够对一个访问账户或一个请求进程占用的资源分配最大限额和最小限额；

——应能够对系统服务水平降低到预先规定的最小值进行检测和报警；

——应提供服务优先级设定功能，并在安装后根据安全策略设定访问账户或请求进程的优先级，根据优先级分配系统资源。

5.9.2.3 关键业务抗抵赖

关键业务抗抵赖技术要求包括：

——系统执行关键业务操作时，对参与者/操作者发生动作时（如：初始录人、修改或数据传递）应加入数字签名功能；宜采用电子签章技术与数字签名技术结合的方式，实现对关键信息或操作的数字签名以及可视化展现；

——系统在敏感信息的传送时，对传送数据进行数字签名，确保消息的发送者或接收者以后不能否认已发送或接收的消息，包括：

- 为数据原发者或接收者提供数据原发证据的功能；
- 为数据原发者或接收者提供数据接收证据的功能；

——应支持对数字签名信息加盖时间戳，时间戳应由国家法定时间源来负责保障时间的授时和守时监测。

5.9.2.4 数据安全传输

数据安全传输包括：

——应对数据交换的参与者双方进行有效的身份认证，应符合 5.9.2.1；

——应对交换数据进行数据完整性保护。宜采用数字摘要、数字签名技术保障数据的完整性；

——应对通信过程中的整个报文或会话过程敏感信息字段进行加密，系统应支持基于标准的加密机制；宜采用 PKI 密码技术或采用具有相当安全性的其他安全机制实现；

——应保障交换数据的真实性及不可抵赖性，应符合 5.9.2.3。

5.9.3 隐私保护服务

隐私保护包括：

——应按照用户的实践范围提供完全符合病人的隐私和保密的要求，包括：

- 应符合 5.9.1.1；
- 应符合 5.9.1.2；
- 应符合 5.9.2.1；

- 应符合 5.9.2.2；
- 应符合 5.9.2.3；
- 应符合 5.9.2.4；
- 应按照用户的实践的范围，提供不同的保密级别；
- 应按照用户的实践的范围进行部分或全部患者病历信息（如用药记录、病历文件）的隐藏功能。

——应提供匿名化服务。保护患者的隐私和安全，确保在区域医疗协同应用子平台中以及提供区域医疗协同以外的传递中使用的患者资料不向非授权用户透露患者的身份；

——应提供许可指令管理服务。转换由立法、政策和个人特定许可指令带来的隐私要求。允许平台用户管理患者/个人的特定许可指示，例如根据法律法规的需要和允许，阻止和屏蔽访问患者病历或者在紧急治疗情况下不经许可直接开放病历信息。

5.9.4 审计追踪服务

审计追踪包括：

——应支持基本的行为审计记录功能，包括：

- 应能够记录每个业务用户的关键操作，例如用户登录、用户退出、增加/修改用户权限、用户访问行为和重要系统命令使用、内部数据访问行为等操作；
- 审计记录的内容应至少包括事件的日期、时间、类型、主体标识、客体标识和结果等；
- 支持授权用户通过审计查阅工具进行审计数据的查询，审计数据应易于理解；
- 具备审计日志数据的完整性保护，应保证审计日志无法删除、修改或覆盖，审计记录应至少保存 6 个月。

——应支持对安全信息的统计分析，包括：

- 能够对业务系统的访问内容、访问行为和访问结果，发现和捕获各种用户访问应用操作行为、违规行为，全面记录业务系统中的各种用户访问会话和事件，实现对业务系统访问信息进行关联分析；
- 系统应支持种类齐全的统计分析策略，并生成多类详尽的安全报告，如日报表、月报表、年报表等阶段报表以及各种比较报表，便于安全管理员从多个角度进行有效的关联分析。

——应支持用户访问行为监测。能够对用户访问平台系统的认证、访问控制、数据签名、数据加密

等业务操作进行综合监控。

6 信息资源规范

6.1 基础信息库

6.1.1 基本要求

基础信息库包括患者基本信息库、医疗卫生人员信息库、医疗卫生机构（科室）信息库和术语和字典信息库。基础信息库是指医疗资源的注册数据，为开展区域医疗协同服务和业务监管提供基础数据支撑。

6.1.2 患者基本信息库

患者基本信息遵循《电子病历基本架构与数据标准（试行）》，应包括该标准的H.02服务对象标识、H.03人口学、H.04联系人、H.05地址、H.06通信、H.07医保等数据组。

6.1.3 医疗卫生人员信息库

医疗卫生人员信息遵循《电子病历基本架构与数据标准（试行）》，应包括该标准的H.09卫生服务者数据组。

6.1.4 医疗卫生机构（科室）信息库

医疗卫生机构（科室）信息遵循《电子病历基本架构与数据标准（试行）》，应包括该标准的 H.08卫生服务机构数据组。

6.1.5 术语和字典信息库

区域医疗协同业务应用子平台术语和字典信息，应支持 WS 363、WS 364、WS 445-2014、《电子病历基本架构与数据标准（试行）》等规范。还应支持GB/T 2261.1、GB/T 2261.2、GB/T 2261.4、GB/T 4658、GB/T 3304、GB/T 14396、ICD-9-CM-3、GB/T 15657、GB/T 16751.3、GB/T 2659。

6.2 区域医疗协同信息库

6.2.1 区域医疗协同服务信息库

区域医疗协同服务信息库的主要内容包括区域医疗协同数据子集、远程会诊数据子集、远程影像诊断数据子集、远程心电诊断数据子集、远程病理诊断数据子集、远程医学教育数据子集、远程预约数据子集、财务管理数据子集等数据子集、双向转诊数据子集、区域医学检验数据子集、区域消毒供应数据子集。

6.2.2 文档存储库

文档存储库应负责将基于活动的、符合标准的临床文档，以明晰、安全和持久的方式进行存储。文档存储库内容应遵循 WS 365-2011、WS 445-2014。

文档存储库依据临床文档的内容类型，选择恰当的文档注册对这些文档进行注册，并对文档检索的请求做出响应。

6.2.3 影像存储库

医疗影像存储要求完全遵循目前国际通用的 DICOM3.0、HL7 等国际标准，符合 IHE 框架，整个系统具有高安全性、高可靠性、较高的兼容性和可持续扩展性。实现影像的接收、中转、打印，支持影像无损与有损压缩存储模式。

6.2.4 文档注册库

文档注册库应提供文档存储库的文档索引信息，内容应包括卫生部《电子病历基本架构与数据标准（试行）》中文档信息模型中文档头的 H.01 文档标示、H.02 服务对象标示、H.03 人口学、H.04 联系人、H.05 地址、H.06 通讯、H.07 医保、H.08 卫生服务机构、H.09 卫生服务者、H.10 事件摘要等数据组的规定。

文档注册库按照临床文档的内容类型，可以存在一组不同类型的注册库，被文档存储库在临床文档存储时使用。

7 IT 基础设施规范

7.1 基本要求

区域医疗协同业务应用子平台采用传统技术架构或云计算技术架构搭建，IT 基础设施（包括基础软件、数据库、服务器、存储和网络等），应满足以下基本技术要求：

——可扩展性要求，应具有良好的横向可扩展性，满足业务系统的处理能力需求；

——可靠性要求，应实现 IT 基础设施各环节的高可靠性，以保障系统稳定可靠运行；

——管理自动化，需要提供标准化的接口以支持监控和管理功能，包括对状态、故障的监控，远程维护等；

——安全性要求，应遵循国内现有标准和规范要求。

7.2 基础软件

7.2.1 应用服务器软件

7.2.1.1 系统基本要求

应用服务器软件应满足以下系统基本要求：

——支持主流操作系统；

——支持主流数据库系统；

——支持主流服务器虚拟化软件系统；

——支持主流消息中间件；

——提供对应用开发的主流框架的支持；

——支持 Web Service 最新标准和规范；

——支持主流备份软件和数据同步软件；

——兼容主流硬件服务器。

7.2.1.2 可扩展性要求

应用服务器软件应满足以下可扩展性要求：

——具有良好的横向扩展能力，实现应用级负载均衡；

——在应用系统不停机的情况下，支持动态增加硬件服务器和应用服务器节点。

7.2.1.3 可靠性要求

应用服务器软件应满足以下可靠性要求：

——应具有容错性，单个应用的部署和故障，不应影响其他应用的部署和运行，不应导致整个系统失效；

——应通过冗余、集群等方式实现高可用性，单节点失效的情况下，可以持续提供服务；

——应实现 HTTP 会话级别的故障恢复；

——在数据库出现故障并恢复情况下，应用服务器应自动恢复数据连接，无需重新启动。

7.2.2 企业基本要求

7.2.2.1 系统基本要求

企业服务总线软件应满足以下系统基本要求：

——支持主流操作系统；

——支持主流数据库系统；

——支持主流服务器虚拟化软件系统；

——支持 Web Service 最新标准和规范；

——支持主流消息中间件；

——提供对应用开放的主流框架的支持，提供主流编程语言的实现接口；

——兼容主流硬件服务器。

7.2.2.2 可扩展性需求

企业服务总线软件应满足以下可扩展性要求：

——具有良好的横向扩展能力，实现负载均衡；

——在企业服务总线不停止服务的情况下，支持动态增加硬件服务器和 ESB 节点。

7.2.2.3 可用性要求

企业服务总线软件应满足以下可用性要求：

——应采用技术来保证平台 7×24h 的运行；

——应保证在数据量或应用连接数高峰运行时的系统运行正常，保障持久化的系统运行。

7.2.2.4 功能需求

企业服务总线软件应满足以下功能要求：

——应遵循 SOA 设计原则和技术标准，提供松耦合模式，实现业务逻辑和应用逻辑、数据逻辑等分离；

——支持智能路由支持，采用灵活的消息路由方式，支持基于消息内容的处理和路由；

——支持标准 XML 数据的格式转换，可通过多种方式实现转换功能；

——提供可靠的数据或消息传输，支持主流消息中间件，支持开放的通讯协议。

7.2.3 数据库管理系统软件

7.2.3.1 系统基本要求

数据库管理系统软件应满足以下系统基本要求：

——支持主流操作系统；

——兼容主流硬件服务器，兼容主流存储架构；

——支持主流的备份软件和数据同步软件；

——兼容主流的应用服务器架构；

——提供对应用开放的主流框架的支持，提供主流编程语言的实现接口。

7.2.3.2 可扩展性要求

数据库管理系统应具有横向可扩展性，支持多节点集群或分布式部署，满足业务的处理能力需求。

7.2.3.3 可用性要求

数据库管理系统应支持以下方式实现系统的高可用性：

——故障恢复；

——多种备份与还原方式；

——基于时间点还原；

——备份压缩；

——数据复制；

——数据库集群或分布式数据库。

7.2.3.4 功能要求

数据库管理系统应满足以下功能要求：

——关系型数据库和对象型数据库应提供对 SQL92 的完全支持以及 SQL99 的核心级别支持；

——应满足数据库事务执行四要素（ACID）：原子性、一致性、隔离性及持久性；

——可选支持以压缩的形式存储数据；

——应支持 Unicode、GBK/GB2312 等多种字符集。

7.2.4 虚拟化软件

区域医疗协同业务应用子平台可采用虚拟化软件，部署虚拟化环境来支撑其他软件和系统的部署和运行。虚拟化软件宜满足以下技术要求：

——虚拟化软件可以支持资源分拆，从逻辑角度而不是物理角度来对资源进行分配和使用，即从单一的逻辑角度来看待不同的物理资源；

——兼容市场上主流的服务器设备，兼容市场主流操作系统和主流的应用软件；

——虚拟机之间应实现相互独立，每个虚拟机之间做到完全隔离，其中某个虚拟机的故障不会影响同一个服务器上其他的虚拟机的运行；

——支持存储虚拟化和网络虚拟化；网络虚拟化需要支持虚拟网络隔离，不通的虚拟机可以处于不同的网络，保证即使位于同一物理服务器上的虚拟机也可以互相隔离；

——支持虚拟机的生命周期管理，包括虚拟机存储信息监控，虚拟网络信息监控和虚拟机的图形化

控制台的查看；

——具备快速部署能力，可以在短时间内完成虚拟系统的搭建，并支持批量创建虚拟机；

——支持动态调度能力；但需要系统节能时，可以通过调度集中虚拟机，并且休眠部分服务器；当某个服务器负载过重时，可以通过调度将虚拟机进行动态迁移，满足负载均衡的需要；上述调度应保证虚拟机内的服务不能停止；

——支持灵活的管理方式；支持对虚拟化系统的远程集中管理，支持基于 Web 方式的平台管理；

——支持在主流分布式文件系统上创建虚拟机。

7.2.5 文件系统

区域医疗协同业务应用子平台可采用文件系统存储居民健康档案文档及其他类型文档。本标准中暂不对文件系统提出具体技术要求。

7.3 硬件服务器

7.3.1 基本要求

区域医疗协同业务应用子平台采用传统技术架构或云计算技术架构搭建，硬件服务器应满足如下技术要求：

——配置合理：服务器的资源配置应尽量与业务需求相匹配，实现资源的均衡使用；

——可扩展性要求：服务器应具有横向和纵向可扩展性，满足业务系统的处理能力需求；

——管理自动化：服务器应提供标准化的接口以支持监控和管理功能，包括对状态、故障、能耗、温度的监控，远程启动、访问和维护等；

——高能效：服务器应具有较高的性能/功耗比，具有良好的散热设计，具有良好的环境适应能力（较宽的温度、湿度范围等），应遵循 HJ2507-2011 的要求。

7.3.2 系统要求

硬件服务器应满足以下系统要求：

——支持主流操作系统；

——采用开放式架构和处理器；

——支持主流的内存型号，内存支持 ECC 纠错；

——支持普通硬盘或固态硬盘，并支持热插拔技术；

——支持磁盘阵列技术；

——支持多种主流存储架构，包括 FC SAN、IP SAN、NAS，可选支持 FCoE 技术；

——系统 I/O 插槽数量及集成网络端口数量可扩展；

——网络接口，应满足以下要求：

- 支持千兆以太网技术，可选支持万兆以太网技术；
- 支持网络端口聚合功能；
- 支持网络端口故障切换功能；
- 可选支持硬件虚拟化辅助技术；
- 可选支持网络加速功能。

——供电：提供单电源/冗余电源可选。

7.3.3 可扩展性要求

服务器系统应满足可扩展性要求，宜采用开放式架构服务器系统，满足平台及应用处理能力需求，包括：

——横向扩展，应满足以下要求：

- 服务器系统应具备主从一定规模的多结点计算系统的能力,提供便利的软硬件部署及管理模式；
- 如果采用云计算技术架构部署，服务器系统应支持动态资源分配和自动化管理。

——纵向扩展，应满足以下要求：

- CPU 扩展能力：在同一主板上支持多个 CPU 插槽，且在提供多个 CPU 插槽的同时支持用户选配 CPU 个数；
- 内存扩展能力：在同一主板上支持多个内存插槽，可通过内存扩展板进行扩展；
- 键盘扩展能力：在一个机箱内支持多块硬盘槽位，应支持 SATA/SAS/SSD 类型硬盘；
- 网卡扩展能力：应提供 2 个或多个千兆以太网卡，可选支持 10Gb 的网络接口；
- 电源扩展能力：一个机箱支持多个电源模块，为主机提供供电保障。

7.3.4 可靠性要求

区域医疗协同业务应用子平台选择主机系统应具备多种可靠性保护措施：

——内存可靠性，主机系统应提供内存保护功能，为需要跟高等级可用性的应用提供增强的容错能力，用户将能够按照自己的意愿来选择系统内存保护级别。具体要求包括：

- 服务器内存提供 ECC 功能；

- 根据内存可靠度要求，可选支持高级 ECC 内存保护技术或内存镜像。

——硬盘可靠性，应满足以下要求：

- 应支持 RAID 技术，保证磁盘系统的高可靠性，提供持续工作而不发生故障的能力，宜包含但不限于：RAID0、1、0+1、5 等级别；
- RAID 卡宜支持缓存电池保护。

——整机可靠性，应满足以下要求：

- 热插拔：用户在不需要切断电源的情况下，对部件进行更换，保证主机正常运行。用户可以安装需求选择不同部件热插拔功能，内存热插拔、硬盘热插拔、PCI-E 热插拔、电源模块热插拔、风扇热插拔等；
- 冗余部件：关键部件（内存、硬盘、电源、风扇等）应提供冗余部件，当一个部件出现故障，另外的部件能支撑主机系统正常运行，故障部件可以进行维护和更换；
- 故障诊断：当主机出现故障时，能够快速定位故障部件，并向管理人员发出报警指令，例如：短信报警、邮件报警、蜂鸣报警等。

7.3.5 虚拟化支持

硬件服务器应满足以下技术要求：

——主机能够支持主流的虚拟化软件；

——所有主机系统应支持同一个虚拟化引擎；

——处理器、I/O 和网络接口应支持虚拟化硬件辅助功能。

7.3.6 服务器可管理性要求

7.3.6.1 总体要求

服务器的管理体系应满足对区域医疗协同业务应用子平台中数量较多的服务器管理要求，便于系统管理员对硬件层面的管理和控制。管理人员应能通过统一接口来管理和监控资产信息、能耗状况、健康状况、性能状况等一系列信息。

7.3.6.2 管理功能要求

服务器应支持独立于操作系统的带外管理功能，包括：

——资产管理，可以获取服务器资产状况，包括型号及序列号、配置信息、固件版本管理；

——配置管理，应满足以下要求：

- 支持将服务器所需软件（操作系统、补丁、应用等）自动分发给该服务器；
- 支持自动执行部署服务器软件，包括自动部署操作系统或者专有的应用。

——远程控制，应支持管理员通过远程的方式来管理和控制，提供健康状况监测和日志查询；可选支持 KVM Over IP，可选支持虚拟介质（如光驱重定向）；

——故障管理，应在服务器前后面板、服务器内部分别提供工作状况指示灯，指示服务器各个部件的工作情况，包括电源、整机健康状况、内部部件（CPU、内存、电源模块、硬盘灯）；刀片服务器应提供刀片机箱及刀片机箱关键部件工作及健康状况指示灯；

——管理接口，应提供独立的管理网口，并支持 IPMI 管理协议、SNMP 管理协议和 SNMP TRAP 机制以及基于 HTTP 的远程管理。

7.4 存储系统

7.4.1 基本要求

存储系统应满足区域医疗协同业务应用子平台目前建设需求及未来发展需求。在满足平台建设需求的前提下，尽量采用优化设计，使数据存储系统能够满足用户需求的高可靠性、高扩展性、异构性、兼容性、易维护性等需求。

存储系统应具备以下特点：

——高可靠性：在系统整体设计中应选用高可靠性存储产品，设备充分考虑冗余、容错能力和备份，同时合理设计存储网络架构，最大限度保障系统正常运行；

——可扩展性：存储网络应支持平滑扩充和升级，避免在系统扩展时对存储网络架构的大幅度调整；

——易管理性：支持集中监控、分权管理，以便统一分配网络存储资源；支持故障自动报警；

——高性能：应保障存储设备的高吞吐能力，保证数据的高质量传输，满足性能要求，避免存储瓶颈影响整体的系统应用；

——先进性和成熟性：存储设备应采用先进的技术和制造工艺；在容量扩展支持、数据空间分配、高性能方面应保持技术领先；网络结构和协议应采用成熟的、普遍应用的并被证明是可靠的结果模型和技术；

——标准的开放性：应支持国际上通用标准的存储协议、国际标准的应用的开放协议，保证与其他主流服务器之间的平滑连接互通和兼容性，以及将来网络的扩展性；

——环保节能：应满足环保与节能的要求，噪声低、耗电低、无污染。

7.4.2 存储可用性要求

存储系统应满足以下可用性要求：

——出现故障及时进行告警（声音、灯闪），告警分等级，界面可见，具有详细说明和修复手段提示；

——要求用户数据可靠性可灵活配置，支持设置用户数据的副本数、是否异地存放，向用户提供不同级别的可靠性保护；

——要求任意两块磁盘或单个存储节点损坏，不会导致用户数据丢失；

——要求任意磁盘或存储节点故障，不影响云存储平台其他设备的正常使用和用户访问；

——产品电位接地，防止触电事故；

——尺寸、规格、形状合理，以免倾斜倒伏，碰撞；

——产品材质耐温，散热；

——明确警示触电、有毒害或其他危险发生的可能。

7.4.3 存储易管理性要求

存储系统应满足以下易管理性需求：

——配有存储管理软件，应实现 FCSAN、IPSAN、NAS 一体化统一管理，提供全中文管理界面；

——支持包括 RS232 串口、10/100M 以太网口、Telnet 方式、图形界面、CLI 命令行等多种管理方式；

——软件内置于存储系统内部，提供的存储管理软件可以在本地或远程设置，管理，监测和调整盘阵的运行；

——支持故障预警功能，提供包括 LED 指示灯报警、蜂鸣报警、Email 报警、日志报警、SNMP 报警等多种报警方式。

7.4.4 存储配置要求

7.4.4.1 概述

由于全国各省市地区人口分布不均，差异巨大。根据人口规模和经济状况，本标准定义了小型、中型、大型三个级别的区域医疗协同业务应用子平台存储要求。建设单位宜根据结合实际情况并参考存储配置要求。

7.4.4.2 小型平台存储配置要求

存储配置宜满足以下要求：

——在线存储要求：

- 关键部件（控制器、电源、风扇等）采用热插拔模块化设计，内部连接无线缆；
- 应支持 IPSAN/FCSAN 存储网络架构，可支持 NAS 异构统一平台，兼容异构存储；
- 可支持 iSCSI、NFS、CIFS 等多种文件共享协议，可安装部署于多种操作系统并存的复杂网络环境中；
- 应支持 iSCSI 主机接口，可支持 FC 主机连接；
- 宜支持 SAS/SATA 硬盘，可支持 SSD/FC 硬盘。实配容量宜≥1TB；最大扩展容量宜≥100TB；
- 大缓存，控制器缓存宜≥16GB，控制器最大缓存宜≥48GB。

——离线存储要求：

- 可选虚拟带库或物理带库设备，支持 LT03\LT04\LT05 驱动器；
- 支持 IP 主机接口，可支持 FC 主机接口；
- 配置容量宜≥10TB，最多支持存储容量宜≥200TB。

7.4.4.3 中型平台存储配置要求

存储配置宜满足以下要求：

——在线存储要求：

- 关键部件（控制器、电源、风扇等）采用热插拔模块化设计，内部连接无线缆；
- 支持 IP SAN/FC SAN 存储网络架构和 NAS 异构统一平台，兼容异构存储，支持存储虚拟化，实现存储资源的整合再利用，提高用户的投资回报率；
- 可支持 iSCSI、NFS、CIFS 等多种文件共享协议，可安装部署于多种操作系统并存的复杂网络环境中；
- 支持 iSCSI、FC 主机连接，无缝接入用户现有应用环境，满足不同客户不同应用对数据存储系统的差异化需求；
- 宜支持 SSD/FC/SAS/SATA 硬盘，支持高转速 FC 磁盘；支持高转速 SAS 磁盘，支持高转速 SATA Ⅱ磁盘，支持 SSD 硬盘。实配容量宜≥6TB；最大扩展容量宜≥180TB，灵活配置满足不同层级数据存储需求；
- 高缓存，控制器缓存宜≥24GB，控制器最大缓存宜≥64GB；
- 异构整合、集中部署，统一管理，降低整体拥有成本（TCO）。

——灾备存储要求。支持本地的连接数据保护功能，存储应具有连续数据保护功能，可以满足数据

恢复要求苛刻的RTO/RPO指标，快速准确的恢复故障前数据。

——离线存储要求：

- 可选用虚拟带库或物理带库设备，支持LTO3\LTO4\LTO5驱动器；
- 支持FC或IP主机接口；
- 配置容量宜≥30TB，最多支持存储容量宜≥300TB。

7.4.4.4 大型平台存储配置要求

存储配置宜满足以下要求：

——在线存储要求：

- 关键部件（控制器、电源、风扇等）采用热拔插模块化设计，内部连接无线缆；
- 支持IP SAN/FC SAN存储网络架构和NAS异构统一平台，兼容异构存储，支持存储虚拟化，实现存储资源的整合再利用，提高用户的投资回报率；
- 支持iSCSI、NFS、CIFS等多种文件共享协议，可安装部署于多种操作系统并存的 复杂网络环境中；
- 支持iSCSI、FC主机连接，无缝接入用户现有应用环境，满足不同客户不同应用对数据存储系统的差异化需求；
- 宜支持SSD/FC/SAS/SATA硬盘，支持高转速FC磁盘；支持高转速SAS磁盘，支持高转速SATA Ⅱ磁盘，支持SSD硬盘。实配容量宜≥16TB；最大扩展容量宜≥400TB，灵活配置满足不同层级数据存储需求；
- 高缓存，控制器缓存宜≥48GB，控制器最大缓存宜≥128GB；
- 异构整合、集中部署，统一管理，降低整体拥有成本（TCO）。

——灾备存储要求：

- 支持本地的连接数据保护功能，存储应具有连续数据保护功能，可以满足数据恢复要求苛刻的RTO/RPO指标，快速准确的恢复故障前数据。
- 支持数据卷隔离映射功能、重复数据删除、自动精简配置、数据快照功能、快照回滚、远程卷复制（同步/异步）、基于快照的远程数据复制远程数据恢复、逻辑分区动态扩容；
- 支持远程容灾功能，结合本地连续数据保护功能，可实现数据级及应用级的容灾。

——离线存储要求：

- 可选用虚拟带库或物理带库设备，支持LTO3\LTO4\LTO5驱动器；

- 支持 FC 或 IP 主机接口；
- 配置容量宜≥60TB，最多支持存储容量宜≥600TB。

7.5 网络系统

7.5.1 区域医疗协同业务应用子平台网络参考架构

本技术规范中的平台网络参考架构在《基于健康档案的医院信息平台建设技术解决方案》基础上，对平台组件构成做了进一步的完善，如表格 15 所示。

表 15

<table>
<tr><td>外联出口区</td><td>业务系统区</td><td>数据区</td><td>数据灾备区</td><td rowspan="2">区域医疗协同业务应用子平台</td></tr>
<tr><td>安全管理区</td><td colspan="2">骨干网络区</td><td>管理接入区</td></tr>
<tr><td>POS1</td><td>POS2</td><td>POS3</td><td>POS4</td><td>POS 接入</td></tr>
</table>

整体网络应由由两大部分组成：

区域医疗协同业务应用子平台网络，主要负责支撑区域医疗协同业务应用子平台的运行和管理，以及与外部系统的连接；

POS 接入，主要负责各 POS 点的接入，实现数据交换和服务调用。

7.5.2 区域医疗协同业务应用子平台区域划分

区域医疗协同业务应用子平台网络按照功能从逻辑上划分，应至少包括以下区域，各区域间需要通过防火墙进行安全隔离。

7.5.2.1 骨干网络区域

该区域主要实现以下功能：

——对各 POS 远程接入链路进行护具；

——连接卫生区域信息平台各区域；

——对卫生区域信息平台各区域数据进行高速转发处理。

7.5.2.2 业务系统区域

该区域主要包括以下业务相关设备：

——应用服务器；

——数据库服务器；

——中间件服务器；

——数据存储设备。

7.5.2.3 EHR 数据区域

该区域主要实现 HER 数据和文档的存储和访问。

7.5.2.4 安全管理区域

该区域主要实现以下功能：

——证书服务器；

——身份认证；

——漏洞扫描；

——入侵检测；

——网络管理。

7.5.2.5 数据灾备区域

该区主要实现以下功能：

——作为远程灾备；

——实现业务系统与灾备区域数据的同步；

——通过高速链路直接与核心交换机。

7.5.2.6 外联出口区

该区域主要实现以下功能：

——负责连接外联单位；

——将来实现域间互连互通时提供开放接口。

7.5.2.7 行政管理接入区

该区域主要负责将相关的行政管理部门接入数据中心。

7.5.2.8 POS－1 接入

POS-1 接入要求：在 POS 的出口有一个文档重构的引擎/适配器（Engine/Adapter）,将内部医疗服务产生的医疗数据转换成标准的业务文档格式，提交到信息平台。

7.5.2.9 POS-2 接入

POS-2 接入要求：采用集中部署的方式，POS 内业务系统通过文档重构的引擎/适配器

（Engine/Adapter），将数据转换成标准的业务文档格式，提交到信息平台。

7.5.2.10 POS-3 接入

POS-3 接入要求：POS 终端设备自身包含的业务应用程序，同时安装文档重构的引擎/适配器（Engine/Adapter），本终端即可产生业务文档，直接提交给信息平台进入业务文档库。

7.5.2.11 POS-4 接入

POS-4 接入要求：终端直接将数据提交给信息平台，由信息平台的业务系统进行文档的重构，提交给业务文档库。

7.5.3 网络带宽要求

7.5.3.1 接入带宽要求

各医疗卫生机构的接入带宽满足以下要求：

——三级医院接入带宽宜≥1000M；

——二级医院接入带宽宜≥100M；

——社区服务中心接入带宽宜≥8M；

——社区服务站接入带宽宜≥4M；

——行政管理接入带宽宜≥100M；

——其它医疗卫生机构应结合业务要求进行配置。

7.5.3.2 区域医疗协同业务应用子平台骨干区域带宽要求

骨干区域带宽宜满足以下要求：

——对于 100 万人口以下的规模的区域，核心交换设备宜达到千兆接入速率；

——对于 100 万人口以上的规模的区域，核心交换设备宜达到万兆接入速率。

7.5.4 骨干网络设计要求

网络可靠性，宜满足以下要求：

——设备级别可靠性要求包括：

- 网络设备支持风扇冗余；
- 网络设备支持电源冗余；
- 核心设备应提供关键部件的冗余备份，关键组件支持热插拔与热备份；
- 核心设备应支持引擎冗余，引擎自动切换；

- 核心设备应支持主流保护技术提高业务恢复能力，实现无中断业务运行。

——网络级别可靠性要求包括：

- 汇聚设备通过两条以上链路与核心设备相连；
- 服务区接入交换机通过两条以上链路与核心设备相连；
- 安全管理区设备通过两条以上链路与核心设备相连；
- 核心设备采用两台或以上进行冗余；
- 核心设备应支持 IP、LDP、VPN、TE 快速重路由；
- 核心设备应支持 Hot-Standby，IGP、BGP 以及组播路由收敛；
- 核心设备应支持 VRRP 协议；
- 核心设备应支持 RRPP 协议；
- 核心设备应支持 TRUNK 链路分担备份；
- 核心设备应支持 BFD 链路快速检测。

7.5.5 服务点系统接入设计要求

网络可靠性，宜满足以下要求：

——支持双出口备份，选择两家不同的运营商提供的物理链路作为互备；

——支持接入设备双机备份；

——支持快速切换，满足以下要求：

- 网关异常时，包括网关瘫痪、重启等需要网关能快速切换；自动侦测特性能够保证在 1S～2S 内发现故障，VRRP 在 3S～4S 内完成主备网关的切换，网关内外都设置 VRRP 组，并将这一对 VRRP 组关联起来；
- 网关链路异常时，需要 VPN 隧道能快速切换。

7.5.6 网络规划要求

IP 地址规划应满足以下要求：

——区域医疗协同业务应用子平台 IP 地址规划要求包括：

- IP 地址的分配应采用 VLSM（Variable Leangth Subnet Mask,变长掩码）技术，保证 IP 地址的利用效率；
- 需采用 CIDR（Classless Inter-Domain Routing，无类别域间路由）技术，这样可以减小路由器路由表的大小。

——在规划 IP 地址时，应结合本地电子政务外网或其它资源网络（如新农合网，社保网）的部署，综合考虑 IP 地址资源分配；

——IP 地址规划，需参照以下标准和规范：

- RFC 0791《因特网协议》；
- RFC 0793《因特控制协议》
- RFC 1366《IP 地址空间管理导则》；
- RFC 1466《IP 地址空间管理导则》；
- RFC 1597 《专用因特网的地址分配》；
- RFC 1918 《专用因特网的地址分配》。

7.5.7 网络管理要求

7.5.7.1 拓扑管理

系统应提供物理拓扑树、IP 视图、时钟视图、隧道视图、自定义视图，用户可以从不同的角度浏览视图，实时了解和监控网络的运行情况。

拓扑管理应支持以下功能：

——拓扑图基础功能包括：

- 鸟瞰图：可方便定位拓扑窗口显示的区域；
- 全网网元统计：可统计全网网元和各种类型网元的数量；
- 拓扑缩放：视图支持缩小和放大；
- 过滤树：可快速过滤出用户关注网元；
- 拓扑视图：需反映网络中的各种物理和逻辑实体，并提供了各种操作的入口。

——支持拓扑告警显示：使用不同的颜色或图标表示子网和网元状态的方式；

——支持拓扑自动发现：系统应提供拓扑自动发现功能，无需人工干预。

7.5.7.2 性能管理

应对网络的关键性能指标进行监控，并对采集到的性能数据进行统计，为用户对网络性能进行管理。性能管理应支持以下几部分功能：

——监控实例管理包括：

- 用户可以按照预先设置的模板和定时策略对指设备的资源进行性能数据收集；
- 监控实例包括数据监控实例和阈值告警监控实例。

——监控模板管理包括：

- 数据监控模板：可对性能指标进行采集，并收集网络资源的性能数据；可以为指标或指标组建立数据监控模板；
- 阈值告警监控模板：可用于采集指定阈值的指标。通过为指定的资源设置阈值告警监控模板，可以监控指定资源的告警。

——历史性能的数据浏览功能包括：

- 网络历史性能数据可以通过拆线图、柱图、图表的方式显示；
- 以多种格式对性能数据进行保存。

7.5.7.3 安全管理

应实现对网管系统本身的安全控制，通过对用户、用户组、权限和操作集等管理，保证网管系统的安全。网管安全管理需支持以下几部分功能：

——登录和会话管理；

——用户和用户组管理包括：

- 新建用户账号和用户组管理；
- 修改用户账号和用户组信息；
- 删除用户账号和用户组。

——权限管理包括：

- 管理权限：用户可以管理的设备范围及其配置数据范围，或者用户所属用户组可以管理的指定区域；在拓扑视图上用户不可管理的设备是不可见的，用户所属用户组不可管理的区域也是不可见的。
- 操作权限：用户可以执行的具体操作。如果一个用户对某一设备没有管理权限，也就不具有该设备的操作权限。

——安全策略管理包括：

- 设置密码策略用来设置用户规则和密码安全策略；
- 密码规则包括普通用户密码长度最小值、超级用户密码最小值和密码长度最大值 ；
- 密码安全策略包括密码不能与历史密码重复次数、密码最长存留天数、密码最短存留天数和密码到期前提前提示天数；
- 设置账户策略用来设置用户名最小长度、自动解锁时间、用户登录时的最大登录尝试次数、

登录或解锁失败延时时间等。

——地址访问控制，限制用户只能从特定的客户端登录服务器。如果客户端需要通过远程方式登陆服务器，应先配置地址访问控制列表。

7.5.7.4 告警管理

应实现对网络中的异常运行情况的实时监控，通过告警统计、定位、提示、重定义、相关性分析、告警远程通知等手段，便于网络管理员及时采取措施，恢复网络正常运行。

告警管理包括需支持以下功能：

——全网告警监控；

——告警统计；

——告警屏蔽和相关分析；

——告警转储和确计；

——告警同步；

——告警重定义：通过告警重定义功能，用户可以根据实际需要重新设置某些告警的级加盟；

——告警跳转：告警定位功能，从告警跳转到产生该条告警的拓扑对象；

——告警维护经验库；

——告警时间本地化：所有告警的产生、确认、清除，到达网管时间均显示网管本地时间；

——多种告警通知手段：支持电子邮件、短消息等告警远程通知。

7.5.7.5 故障管理

故障采集应支持如下类型：

——硬件类问题；

——系统类问题；

——二层网络问题；

——三层网络及路由问题；

——组播问题；

——接口对接问题；

——QoS 问题。

故障采集应支持以下几种方式：

——支持直连方式：管理终端与待采集设备可通过网络或者串口线直接相连，通过 Telnet、SSH

或串口方式连接设备；

——支持自动代理方式：能够确定代理的设备类型时，选用自动代理；

——支持手工代理方式：不能确定代理的设备类型时，选用手工代理；

——支持 VPN 实例方式：设备位于 VPN 私网中，选用 VPN 实例方式。

7.5.7.6 报表管理

网络管理系统应实现针对 IT 资源的监控参数，根据管理人员的要求制定周期性的参数监控并产生相应的报表。系统应产生以下基础类型报表：

——告警和日志类报表，包括：

- 设备告警级别分布明细报表；
- 设备告警级别分布报表；
- 设备通断统计报表；
- 通用告警信息报表；
- 历史变更记录报表。

——资源类报表，包括：

- 端口资源统计报表；
- 以太网端口资源统计报表；
- 以太网网元间业务资源统计报表；
- 组网图。

7.5.7.7 日志分析

系统应支持通过对设备日志进行分析，实现对日志的结构化显示，并支持对重要信息的过滤搜索等功能。

日志分析应支持的功能包括：

——文件操作：日志文件的打开、保存；

——配置管理：为选择的日志文件配置解释库，以便在解释栏输出选中的日志对应的解释信息；

——日志记录列显示、列隐藏；

——日志记录排序：使当前页中的日志记录按照指定的方式进行排序；

——日志记录批注：提供批注的插入、编辑、浏览和删除功能；

——搜索功能：包括对当前页、当前文件、所有文件进行搜索；用户可以根据关键字进行搜索；

——过滤功能：只显示带有用户所选指定项的日志记录，其它日志记录被隐藏。

7.5.7.8 网络巡检

系统应依据网络 IT 设备的巡检检查列表、相关预警及专家的经验，对设备配置和日常运行情况进行定期巡检和维护。对于设备中不符合规范的配置和出现的问题，巡检工具应给出相应的报告和提示信息，同时提供处理意见和措施。

——巡检应包含以下项目：

- 设备单板版本的预警信息；
- 版本及补丁是否规范使用；
- 设备基本配置；
- 业务模块运行是否正常；
- 接口状态检查；
- 路由配置及状态；
- 系统异常情况；
- 芯片级协议级的状态检查。

——巡检安排，包括：

- 例行巡检；
- 重大节日巡检，在春节、国庆节等重要节日前应有针对性地对重点网络进行巡检，并给出详细分析和整改建议；
- 升级后健康检查，在升级观察期内，应定期使用巡检工具登录进行巡检和观察，监控设备和版本的运行情况，防止新问题出现。

7.5.7.9 备件管理

管理管理功能包括：

——基础数据管理，包括：

- 替换关系管理：管理最新的产品单板替代关系；
- 统计数据管理：管理最新的备件统计基础数据；
- 整机清单数据管理：管理最新的整机清单数据。

——管理管理，包括：

- 备件查询：进行备件信息查询；

- 单项备件统计：根据现网的单项备件数量，统计需要的单项备件数量；
- 批量备件统计：根据现网的备件数量，需要批量统计备件数量；
- 数据导出：查询统计任务的数据结果导出并保存。

7.6 灾备要求

应在生产系统外创建生产系统数据的副本，以满足灾难备份的要求。应通过技术手段实现生产系统和灾备系统之间的数据镜像或复制。灾备系统的建设应遵循 GB/T20988-2007 的要求。

灾备建设的指标主要为 RPO 和 RTO 两种：

——RPO（Recovery Point Objective）恢复点目标：指一个过去的时间点，当灾难或紧急事件发生时，数据可以恢复到的时间点。

——RTO（Recovery Time Object）恢复时间目标：是指灾难发生后，从 IT 系统宕机导致业务停顿之刻开始，到 IT 系统恢复至可以支持各部门运作，业务恢复运营之时，此两点之间的时间段成为 RTO。

RTO/RPO 与灾难恢复能力等级的关系宜参考表 16。

区域医疗协同业务应用子平台作为区域医疗的重要信息平台，不论规模大小，都应该规划实现 4 级以上灾备等级。

对于基本规模区域医疗协同业务应用子平台，灾难备份系统的建设目标是 RPO 为数小时至 1D，RTO 为数小时至 2D。

对于中级规模区域医疗协同业务应用子平台，灾难备份系统的建设目标是 RPO≤30min，RTO 为数分钟至 2H。

对于高级规模区域医疗协同业务应用子平台，灾难备份系统的建设目标是，灾难发生后数据不容丢失，即 RPO=0，RTO 为数分钟。

表 16 RTO/RPO 与灾难恢复能力等级的关系

灾难恢复能等级	RTO	RPO
1	≥2d	1d～7d
2	≥24H	1d～7d
3	≥12H	数小时～1d
4	数小时～2d	数小时～1d
5	数分钟～2H	0 min～30 min

6	数分钟	0 min

7.7 可管理性要求

7.7.1 基本要求

区域医疗协同业务应用子平台提供的 IT 基础设施各个组件（服务器、存储、网络等）应满足可管理性要求；区域医疗协同业务应用子平台作为服务平台，也应满足可管理型的要求。

7.7.2 服务级别协议

区域医疗协同业务应用子平台的服务提供者将为区域内相关医疗卫生机构提供从硬件到软件的服务。服务提供者应该和服务使用者约定服务级别协议（SLA）。SLA 应规范的内容如下（包括且不限于）：

——分配给客户的最小带宽；

——客户宽带极限；

——能同时服务的客户数目；

——在可能影响用户行为的网络变化之前的通知安排；

——系统可用性；

——收费依据。

7.7.3 服务申请及变更

平台服务的使用者可以透过平台申请所需的服务，应满足如下要求：

——用户可以通过交互接口请求服务；平台的所有服务目录存放在服务目录里，用户可以通过门户或接口方式请求相关服务；

——系统能够对不同渠道提交的事件进行记录、转发、配置、部署、跟踪和反馈等工作；

——使用者所需服务内容和范围发生变更，或服务的提供方所提供的服务发生变化，平台能够提供服务变更流速，记录、审批并实施服务的变更。

7.7.4 配置/部署管理

配置/部署管理应包括：

——实现自动化部署。平台按照业务的要求，能够对虚拟资源、应用系统、配置变更等内容实施自动化部署。最大程序减少人工干预带来的不确定性和低效率。

——配置相对充足的虚拟化资源，保证资源的弹性及动态扩展。平台随时报告资源的可用情况，并保持一定的可用资源，以便增添新的业务及应用业务高峰。

——通过定制的工作流自动完成需要手工完成的配置和部署的过程。

7.7.5 监控

对于任何环境而言，监控资源和应用程序性能都是非常重要的环节。在虚拟化环境中，监控任务更为困难，也更为关键。系统应实现：

——采集服务器、服务器集合、网络、存储等实时数据，反应资源使用情况；

——校验服务级别协议（SLA）的符合性；

——自动生成系统资源警告及详细数据，方便快速检测和解决应用程序问题；

——报告应用程序的资源使用情况数据；

——提供一站式门户网站查看每个受监控资源的详细信息。

7.7.6 容量规划

区域医疗协同业务应用子平台内的系统、软件和数据容量将不粘增长。应可以监控现有资源使用情况，并追溯历史数据来预测未来容量需求趋势。

7.7.7 事件管理

平台服务的提供者，应提供相应的事件管理功能，记录发生事件、内容及处理过程，包括：

——事件的时间；

——事件的级别；

——事件的内容；

——事件的状态。

7.7.8 资产管理

应提供 IT 基础设备资产管理功能，满足资产审计、折旧、变更、淘汰等管理要求。

8 安全规范

8.1 安全设计原则

8.1.1 规范性原则

区域医疗协同业务应用子平台应安装信息系统等级保护三级（或以上）的要求进行安装建设，安全设计应遵循已颁布的相关国家标准。

8.1.2 先进性和适用性原则

安全设计应采用先进的设计思想和方法，尽量采用国内外先进的安全技术。所采用的先进技术应符合实际情况；应合理设置系统功能、恰当进行系统配置和设备选型，保障其具有较高的性价比，满足业务管理的需要。

8.1.3 可扩展性原则

安全设计应考虑通用性、灵活性，以便利用现有资源及应用升级。

8.1.4 开放性和兼容性原则

对安全子系统的升级、扩充、更新以及功能变化应有较强的适应能力。即当这些因素发生变化时，安全子系统可以不做修改或少量修改就能在新环境下运行。

8.1.5 可靠性原则

安全设计应确保系统的正常运行和数据传输的正确性，防止由内在因素和硬件环境造成的错误和灾难性故障，确保系统可靠性。在保证关键技术实现的前提下，尽可能采用成熟安全产品和技术，保证系统的可用性、工程实施的简便快捷。

8.1.6 系统性原则

应综合考虑安全体系的整体性、相关性、目的性、实用性和适应性。另外，与业务系统的结合相对简单且独立。

8.1.7 技术和管理相结合原则

安全体系应遵循技术和管理相结合的原则进行设计和实施，各种安全技术应该与运行管理机制、人员思想教育与技术培训、安全规章制度建设相结合。从社会系统工程的角度综合考虑，最大限度发挥人防、物防、技防相结合的作用。

8.2 总体框架

总体框架的设计要求包括：

——应从安全技术、安全管理为要素进行框架设计；

——应从网络安全（基础网络安全和边界安全）、主机安全（终端系统安全、服务端系统安全）、应用安全、数据安全几个层面实现安全技术类要求；

——应从安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理几个层面实现安全管理类要求。

8.3 技术要求

8.3.1 物理安全

物理安全主要是指区域医疗协同业务应用子平台所在机房和办公场地的安全性，主要应考虑以下几个方面内容：

——物理位置的选择，应满足 GB/T22239-2008 中 7.1.1.1 的要求；

——物理访问控制，应满足 GB/T22239-2008 中 7.1.1.2 的要求；

——防盗窃和防破坏，应满足 GB/T22239-2008 中 7.1.1.3 的要求；

——防雷击，应满足 GB/T22239-2008 中 7.1.1.4 的要求；

——防火，应满足 GB/T22239-2008 中 7.1.1.5 的要求；

——防水和防潮，应满足 GB/T22239-2008 中 7.1.1.6 的要求；

——防静电，应满足 GB/T22239-2008 中 7.1.1.7 的要求；

——温湿度控制，应满足 GB/T22239-2008 中 7.1.1.8 的要求；

——电力供应，应满足 GB/T22239-2008 中 7.1.1.9 的要求；

——电磁防护，应满足 GB/T22239-2008 中 7.1.1.10 的要求。

8.3.2 网络安全

8.3.2.1 基础网络安全

8.3.2.1.1 结构安全

结构安全技术要求包括：

——应保证主要网络设备的业务处理能力具备冗余空间，满足业务高峰期需要；关键网络设备的业务处理能力至少为历史峰值的 3 倍；

——应保证网络各个部分的带宽满足业务高峰期的需要；

——应绘制与当前运行情况相符完整的网络拓扑结构图，有相应的网络配置表，包含设备 IP 地址等主要信息，与当前运行情况相符，并及时更新；

——网络系统建设应符合 7.5 要求。

8.3.2.1.2 网络设备防护

网络设备防护技术要求包括：

——应对登录网络设备的用户进行身份鉴别；

——应删除默认用户或修改默认用户的口令，根据管理需要开设用户，不得使用缺省口令、空口令、

弱口令；

——应对网络设备的管理员登录地址进行限制；

——网络设备用户的标识应唯一；

——身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换；

——应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；

——当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。

8.3.2.2 安全区域边界安全

安全区域边界安全技术要求包括：

——在区域医疗协同业务应用子平台和外部网络边界处应部署防火墙设备或其他访问控制设备，访问控制设备需具备以下功能：

- 实现基于源/目的的 IP 地址、源 MAC 地址、服务/端口、用户、时间、组（网络、服务、用户、时间）的精细粒度的访问控制；
- 应设定过滤规则集，规则集应涵盖对所有出入边界的数据包的处理方式；
- 能对连接、攻击、认证和配置等行为进行审计，并且可以对升级事件提供的告警；
- 实现日志的本地存储、远端存储、备份等存储方式；
- 应对进出网络的信息内容进行过滤，实现对应用层 HTTP、FTP、TELNET、SNMP、POP3 等协议命令级的控制；
- 应在会话处于非活跃一定时间或会话结束后终止网络连接；
- 重要网段应采取技术手段防止地址欺骗；应禁用网络设备的闲置端口，采用对非虚拟 IP 进行设备地址绑定等方式防止地址欺骗。

——在平台和外部网络边界部署检测设备实现探测网络入侵和非法外联行为，检测控制设备需具备以下功能：

- 能够监测以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等；
- 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警；
- 应能够对内部网络用户私自联到外部网络的行为进行检查，准确定出位置，并对其进行有

效阻断；

- 能够检查网络用户终端采用双网卡跨接外部网络，或采用电话拨号、ADSL 拨号、手机、无线上网卡等无线拨号方式连接其他外部网络。

——应在平台和外部网络边界处对恶意代码进行检测和清除，包括：

- 在不严重影响网络性能和业务的情况下，应在网络边界部署恶意代码检测系统；
- 如果部署了主机恶意代码检测系统，可选择安装部署网络边界恶意代码检测系统。

8.3.2.3 安全审计

在平台和外部网络边界处部署审计系统，收集、记录边界的相关安全事件，并将审计记录转换为标准格式，上报审计管理中心。边界审计系统需具备以下功能；

——收集、记录网络系统中的网络设备运行状况、网络流量、用户行为的日志信息；

——审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

——支持使用标准通讯协议将探测到的各种审计信息上报审计管理中心；

——应能够根据记录数据进行分析，并生成审计报表；

——应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。

8.3.3 服务端系统安全

8.3.3.1 身份鉴别

通过使用安全操作系统或相应的系统加固软件实现用户身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检测以及登录失败处理功能，并根据安全策略配置相关参数，安全操作系统或系统加固软件需具备以下功能：

——在每次用户登录系统时，采用强化管理的口令或具有相应安全强度的其他机制进行用户身份鉴别，并对鉴别数据进行保密性和完整性保护，要求包括：

- 宜支持数字证书+USB KEY 的认证方式实现强身份鉴别；
- 配置用户名/口令认证方式时，口令设置应具备一定的复杂度，不合格的口令被拒绝；口令应具备采用 3 种以上字符、长度不少于 8 位，并设置定期更换要求。

——应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证系统中不存在重复用户身份标识，身份鉴别信息不易被冒用；

——应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；

——当对服务器进行远程管理时，应采取不要措施，防止鉴别信息在网络传输过程中被窃听；

——应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别，包括：

- 通过本地控制台管理主机设备时，应采用一种或一种以上身份鉴别技术；
- 以远程方式登录主机设备，应采用两种或两种以上组合的鉴别技术进行身份鉴别。

8.3.3.2 访问控制

通过使用安全操作系统或相应的系统加固软件进行系统加固实现自主访问控制安全要求。安全操作系统或系统加固软件需具备以下功能：

——策略控制：能接收到管理中心下发的安全策略，并能依据此策略对登录用户的操作权限进行控制；

——客体创建：用户可以在管理中心下发的安全策略控制范围内创建客体，并拥有对客体的各种访问操作（读、写、修改和删除等）权限；

——授权管理：用户可以将自己创建的客体的访问权限（读、写、修改和删除等）的部分或全部授予其他用户；

——访问控制主体的粒度为用户级，客体的粒度为文件或数据库表级；

——应对重要信息资源设置敏感标记；

——应依据安全策略严格控制用户对敏感标记重要信息资源的操作；

——应对重要服务器进行监视，包括监视服务器的 CPU、硬盘、内存、网络等资源的使用情况；

——应能对系统的服务水平降低到预先规定的最小值进行检测和报警。重要服务器的 CPU 利用率、内存、磁盘存储空间等指标超过预先规定的阈值后应进行报警。

8.3.3.3 安全审计

在管理区域部署审计系统，对区域卫生平台范围内的主机探测、记录、相关安全事件，实现系统安全审计。审计系统需具备以下功能：

——审计范围应覆盖到服务器上的每个操作系统用户和数据库用户；

——审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件；审计内容至少包括：用户的添加和删除、审计功能的启动和关闭、审计策略的调整、权限变更、系统资源的异常使用、重要的系统操作（如用户登录、退出）等；

——审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；

——应保护审计记录，避免受到未预期的删除、修改或覆盖等；审计记录应至少保存 6 个月；

——应能够根据记录数据进行分析，并生成审计报表；

——应保护审计进程，避免受到未预期的中断。

8.3.3.4 恶意代码防范

通过部署病毒防护系统或配置具有相应功能的安全操作系统，实现主机计算环境的病毒防护以及恶意代码防范，病毒防护系统需具备以下功能：

——远程控制与管理；

——保持操作系统补丁及时得到更新；

——全网查杀毒；

——防毒策略的定制与分发实时监控；

——客户端防毒状况；

——病毒与事件报警；

——病毒日志查询与统计；

——集中式授权管理；

——全面监控邮件客户端。

8.3.3.5 剩余信息保护

剩余信息保护技术要求包括：

——应保证操作系统和数据库系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清楚，无论这些信息是存放在硬盘上还是在内存中；

——应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。

8.3.3.6 入侵防范

入侵防范技术要求包括：

——操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新；

——应能够监测到对重要服务器进行入侵的行为，能够记录入侵的源 IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；

——应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施，如不能正常恢复，应停止有关服务，并提供报警。

8.3.4 终端系统安全

通过使用安全操作系统或相应的系统加固软件进行系统加固实现终端系统安全加固。安全操作系统或系统加固软件或硬件需具备以下功能：

——应对登录终端操作系统的用户进行身份标识和鉴别，宜支持数字证书进行身份认证，使用口令进行身份认证时，口令应有复杂度要求并定期更换；

——应依据安全策略控制用户对资源的访问，禁止通过 USB、光驱等外设进行数据交换，关闭不必要的服务和端口等；

——应对系统中的重要终端进行升级，审计粒度为用户级；

——审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用及其他与审计相关的信息；

——审计记录至少应包括事件的日期、时间、类型、用户名、访问对象、结果等；

——应保护审计进程，避免受到未预期的中断；

——应保护审计记录，避免受到未预期的删除、修改或覆盖等，审计记录至少保存 3 个月；

——应定期对审计记录进行分析，以便及时发现异常行为；

——操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并保持系统补丁及时得到更新；

——宜支持多操作系统，分离不同类型的应用场景；

——可以采用硬件加固的方式实现终端系统安全加固，隔离异常终端，并且实现数字内容版权保护。

8.3.5 应用安全

应用安全技术要求包括：

——用户管理和权限控制，应符合 5.9.1；

——信息安全，应符合 5.9.2；

——隐私保护，应符合 5.9.3；

——审计追踪，应符合 5.9.4；

——剩余信息保护，包括：

- 应保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；
- 应保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他

用户前得到完全清除；

——软件容错，包括：

- 应提供数据有限性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求；
- 在故障发生时，应用系统应能够继续提供一部分功能，确保能够实施必要的措施。

8.3.6 数据安全备份恢复

数据安全及备份恢复技术要求包括：

——应能检测到系统管理数据、身份鉴别信息、电子健康档案和电子病历等重要业务数据在传输和存储过程中完整性受到破坏，并能够采取必要的恢复措施，包括：

- 宜采用数字摘要技术保障数据的完整性；
- 宜采用数字签名/验签技术、时间戳技术保障数据的真实性及不可抵赖性；
- 能对发现的数据破坏事件进行记录；

——应对身份鉴别信息、电子健康档案和电子病历等重要业务数据在传输和存储过程中对敏感信息字段进行加密，系统应支持基于标准的加密机制；宜采用 PKI 密码技术或采用具有相当安全性的其他安全机制实现；

——应建立数据备份措施，建立备份管理制度，制定数据备份策略，对重要信息进行备份以及对依据备份记录进行数据恢复，具体要求包括：

- 定期采取手工备份方式对重要文件及保存在数据库中的数据进行备份；
- 定期采取自动备份系统镜像应用数据备份，管理员应复核自动备份结果；
- 关键存储部件宜采用冗余磁盘阵列技术并支持失效部件的在线更换；对重要设备应进行冗余配置，以实现双机热备或冷备；
- 数据库服务器宜采用双机冗余热备方式；进行定期在线维护，以缩短恢复所需时间；
- 用户可以通过备份记录进行数据恢复；
- 在条件具备的情况下，应在异地建立和维护重要数据的备份存储系统，利用地理上的分离保障系统和数据对灾难性事件的抵御能力；
- 故障恢复前制定合理的恢复工作计划以及故障恢复方案，数据恢复完成后应检测数据的完整性。

8.4 管理要求

基本管理要求从安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理几个方面提出，具体包括：

——安全管理制度，应满足 GB/T22239-2008 中 7.2.1 的要求；

——安全管理机构，应满足 GB/T22239-2008 中 7.2.2 的要求；

——人员安全管理，应满足 GB/T22239-2008 中 7.2.3 的要求；

——系统建设管理，应满足 GB/T22239-2008 中 7.2.4 的要求；

——系统运维管理，应满足 GB/T22239-2008 中 7.2.5 的要求。

9 机构接入规范要求

机构接入规范内容应包括以下部分：

——功能服务接入规范：医疗机构应实现注册服务、区域医疗协同数据资料整合服务、区域医疗协同数据资料管理服务、区域医疗协同数据资料调阅服务、区域医疗协同结果信息反馈服务、评价安全与隐私服务接口；

——信息服务接入规范：医疗机构应实现个人基本信息、电子病历文档信息、医疗服务信息、疾病管理信息等服务接口；

——机构数据采集接口规范：应遵循 WS 363-2011、WS 364-2011、WS 365-2011、WS 445-2014，例如医院信息平台交互规范、区域卫生信息平台交互规范等。

9.1 功能服务接入规范

9.1.1 注册服务调用

医院信息平台或医院信息系统在进行医疗卫生人员、医疗卫生机构、术语和字典登记及区域医疗协同申请时，应调用区域医疗协同业务应用子平台的注册服务，以实现区域医疗协同信息共享和业务协同。

9.1.2 区域医疗协同数据资料整合服务调用

医院信息平台或医院信息系统通过调用区域医疗协同业务应用子平台区域医疗协同数据资料整合服务，实现医院信息平台电子病历相关数据的抽取、转换和加载，或者按照区域医疗协同业务应用子平台的规范要求开放相关接口给区域医疗协同业务应用子平台调用。

9.1.3 区域医疗协同数据资料管理服务调用

区域医疗协同应用系统通过调用区域医疗协同业务应用子平台区域医疗协同数据资料管理服务，实

现对区域医疗协同数据资料的数据质量核查与反馈。

9.1.4 区域医疗协同数据资料调阅服务调用

区域医疗协同应用系统通过调用区域医疗协同业务应用子平台区域医疗协同数据资料调阅服务，根据平台分配的患者唯一标识 ID，查询并获取患者的区域医疗协同数据资料，以实现区域医疗协同数据资料共享利用。

9.1.5 区域医疗协同结果信息反馈服务调用

区域医疗协同应用系统通过调用区域医疗协同业务应用子平台区域医疗协同结果信息反馈服务，将区域医疗协同服务结果信息提交至区域医疗协同业务应用子平台，平台根据订阅发布机制，将区域医疗协同服务结果信息发布给订阅者。

9.1.6 安全与隐私服务接口

区域医疗协同应用系统通过调用安全与隐私服务安全的提交和使用区域医疗协同数据资料。

9.2 信息服务接入规范

医疗卫生机构开展区域医疗协同服务时，区域医疗协同数据资料上传服务调用如表 17 所示。

表 17 区域医疗协同数据资料上传服务调用

序号	服务名称	服务描述
1	区域医疗协同申请信息接收服务调用	上传患者的自然信息、就诊信息及申请会诊信息；应包含患者 ID、姓名、性别、出生日期、身份证号、职业、联系方式、就诊医院、就诊科室、就诊时间、接诊医师、拟申请区域医疗协同医疗机构、区域医疗协同时间等
2	病案首页信息接收服务调用	包括患者的自然信息、就诊信息、诊断信息、手术信息等
3	医嘱信息接收服务调用	包括患者基本信息、医嘱开立时间、医嘱内容、频率、用法、用量、总量等
4	处方信息接收服务调用	包括患者基本信息、疾病诊断信息、药物名称、药物规格、使用次计量、使用次计量单位、频次等
5	入院记录文档接收服务调用	包括患者基本信息、主诉、现病史、既往史、家族史、体格检查等

6	病程记录文档 接收服务调用	包括患者基本信息、主诉、病例特点、诊断依据、诊断信息等
7	手术记录文档 接收服务调用	包括患者基本信息、手术时间、手术诊断、手术诊断、手术名称、手术指导者、手术者及助手姓名、麻醉方法、手术经过、术中出现的情况及处理等
8	检查报告 接收服务调用	包括患者基本信息、诊断信息、检查部位、检查方法、检查项目、检查日期、检查报告结果等
9	检验数据 接收服务调用	包括患者基本信息、检验日期、检验项目、标本信息、检验结果、检验设备等
10	影像资料 接收服务调用	包括标准的 DICOM3.0 文件，以及索引信息等
11	病理文档 接收服务调用	将病理切片转换成 JPEG、JPEG2000 或 DICOM 格式的数字切片
12	心电数据 接收服务调用	XML 格式的数字心电图数据，包括患者基本信息、数字化存储、采样率、采集长度、数据导联等
13	病历摘要文档 接收服务调用	患者就诊期间的临床摘要文档上传
14	完整电子病历文档 接收服务调用	一次性上传患者就诊期间产生的完整电子病历文档

10 性能要求

规定区域医疗协同业务应用子平台的性能指标要求。

10.1 最小并发用户数

对于区域医疗协同业务应用子平台的服务，最小并发用户数要求：

——接入一个基层医疗机构，允许最小并发用户数大于或等于 10 个；

——接入一个二级医疗机构，允许最小并发用户数大于或等于 50 个；

——接入一个三级医疗机构，允许最小并发用户数大于或等于 100 个。

10.2 基础服务平均相应时间性能

基础服务平均相应时间要求包括：

——患者注册服务调用，单个患者信息注册平均响应时间小于 1 s；

——区域医疗协同数据查询，按照患者唯一标识查询，返回患者区域医疗协同数据文档目录树时，平均响应时间小于 2 s；

——患者基本信息查询，总记录 50 万以上，按照患者唯一标识查询患者基本信息，平均响应时间小于 2 s；总记录 100 万以上，平均响应时间小于 3 s；

——基于人口统计学信息的患者信息匹配（基于索引），总记录 50 万以上，返回患者唯一标识数据，返回记录小于 10 条时，平均响应时间小于 5 s；总记录 100 万以上，返回记录数小于 10 条时，平均响应时间小于 10 s。

10.3 区域医疗协同数据资料交换服务性能

区域医疗协同数据资料交换服务性能要求包括：

——单记录交换/入库的平均响应时间≤20 ms；

——批量数据上传：峰值 800 笔/min。

10.4 区域医疗协同数据资料调阅服务性能

区域医疗协同数据资料调阅服务性能要求包括：

——千万级数据量下单记录本地查询的响应时间≤3 s；

——千万级数据量下分布式查询的响应时间≤5 s。

10.5 区域医疗协同业务协同服务性能

区域医疗协同业务协同服务性能要求包括：

——区域医疗协同数据资料业务协同服务响应：峰值 30 笔/s；

——区域医疗协同数据资料业务协同接收服务请求时间≤2 s；

——区域医疗协同数据资料业务协同发送业务服务时间≤5 s。

10.6 网络性能要求

10.6.1 路由器性能要求

——支持 IPSec VPN 和 GRE VPN；

——支持信息中心监控设备：提供单板管理、电源管理、风扇管理、电子标签的信息监控功能；

——支持版本管理：提供在线版本升级、回退、补丁加载功能；

——支持镜像监控设备：提供基于端口和基于流分类的镜像功能；

——对于无线路有器需支持远程 POE 供电：提供基于 LAN 侧的以太远程供电功能。

10.6.2 交换机性能要求

——以太网接口可支持 10M、100M、1000M、10G 和自协商速率；

——支持接口流量控制，接口隔离、接口转发限制；

——支持广播风暴抑制；

——支持日志、告警、调试信息统一管理；

——支持设备自动加入集群；

——支持预防控制报文攻击；

——提供接口镜像、流镜像；

——支持 NAT 地址池、NAT 多实例；

——支持 AH 和 ESP 两种 IPSec VPN 模式。

10.6.3 防火墙性能要求

——支持源 NAT、目的 NAT、源 PAT、目的 PAT 地址转换；

——可防范多种 DoS 攻击，包括 SYN Flood、ICMP Flood、UDP Flood、WinNuke、ICMP 重定向和不可达报文、Land、Smurf、Fraggle 等；

——可防范扫描窥探，包括地址扫描、端口扫描、IP 源站选路选项、IP 路由记录选项、ICMP 探测报文；

——支持电源 1+1 备份，支持电源热插拔；

——支持动态加载热补丁；

——支持基于应用层的流量控制，优先转发等 QOS 策略，保证重要的应用优先转发。

10.6.4 入侵检测性能要求

——需支持分级管理，实现分布式部署、统一管理；

——可远程设置探测引擎环境、入侵检测规则及响应方式；

——要求实时跟踪当前的代码攻击；

——能够检测各种应用层攻击，包括但不限于：后门程序，木马程序，间谍软件，蠕虫，僵尸主机，异常代码，协议异常，扫描，可疑行为审计类等；

——能够对跨站攻击、SQL 注入等 WEB 攻击行为进行有效检测。