ICS 11.020
C 07

WS

中 华 人 民 共 和 国 卫 生 行 业 标 准

WS XXXXX—2012

基于电子病历的医院信息平台技术规范

Technical specification for Hospital Information Platform based on EMR

（征求意见稿）

2012－XX－XX 发布　　2012－XX－XX 实施

中华人民共和国卫生部　发布

目　　次

前　言

本标准由卫生部统计信息中心提出并归口。

本标准起草单位

本标准主要起草人：

引　言

《基于电子病历的医院信息平台技术规范》是规范基于电子病历的医院信息平台建设的技术规范，对医院信息平台建设开展测试、验收和评价工作提供指导。

本规范的第4章，描述了医院信息平台的整体架构，提出了医院信息平台的整体技术要求；第5章，提出了医院信息平台的基本功能要求；第6章，针对医院信息平台信息资源中心提出数据规范要求；第7章，提出了医院信息平台与区域卫生信息平台以及各类临床信息系统的交互规范；第8章，对医院信息平台的基础设施建设提出技术要求；第9章，提出了医院信息平台的安全规范；第10章，提出了医院信息平台基础服务的性能要求。

基于电子病历的医院信息平台技术规范

1 范围

本规范规定了医院信息平台的总体技术要求、平台基本功能要求、信息资源规范、交互规范、IT基础设施规范、安全规范和性能要求等。本规范不包括基于医院信息平台的应用系统（如居民健康卡、计算机化医嘱录入、智能电子病历编辑器、电子病历浏览器、区域医疗卫生协同、管理辅助决策支持、临床辅助决策支持和患者公众服务）以及接入医院信息平台的医院业务系统（临床服务系统、医疗管理系统、运营管理系统等）应遵循的功能和技术要求。

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。

GB 3304-1991 中国各民族名称的罗马字母拼写法和代码

GB/T 15657—1995 中医病证分类与代码

GB/T 16751.3-1997 中医临床诊疗术语治则治法部分

GB/T 20988-2007 信息系统灾难恢复规范

GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求

GB/T 2261.1-2003 个人基本信息分类与代码 第1部分 人的性别代码

GB/T 2261.2-2003 个人基本信息与分类代码 婚姻状况代码

GB/T 2261.4-2003 个人基本信息分类与代码 第4部分 从业状况(个人身份)代码

GB/T 2659-2000 世界各国和地区名称代码

GB/T 4658-1984 文化程度代码

WS XXXX—2012 电子病历基本数据集

WS XXXX—2012 基于居民健康档案的区域卫生信息平台技术规范

电子病历基本架构与数据标准（试行）（卫办发［2009］130号）

疾病分类与代码（修订版）（卫办综发［2011］166 号）

基于电子病历的医院信息平台建设技术解决方案（1.0版）（卫办综发〔2011〕39号）

3 术语、定义和缩略语

3.1 术语和定义

3.1.1

电子病历 electronic medical record

电子病历是由医疗机构以电子化方式创建、保存和使用的，重点针对门诊、住院患者（或保健对象）临床诊疗和指导干预信息的数据集成系统，是居民个人在医疗机构历次就诊过程中产生和被记录的

完整、详细的临床信息资源，是记录医疗诊治对象医疗服务活动记录的信息资源库，该信息资源库以计算机可处理的形式存在，并且能够安全的存储和传输，医院内授权用户可对其进行访问。

3.1.2

基于电子病历的医院信息平台 hospital information platform based on electronic medical record

基于电子病历的医院信息平台（以下简称医院信息平台），以患者电子病历的信息采集、存储和集中管理为基础，连接临床信息系统和管理信息系统的医疗信息共享和业务协作平台，是医院内不同业务系统之间实现统一集成、资源整合和高效运转的基础和载体。医院信息平台也是在区域范围支持实现以患者为中心的跨机构医疗信息共享和业务协同服务的重要环节。

3.1.3

信息资源中心 information resources center

以电子病历为核心整合医院临床服务、医疗管理、运营管理等数据，形成全院级的数据存储和管理中心，为医院业务应用系统以及医院管理辅助决策、医院临床辅助决策和临床教学和科研提供信息服务。

3.1.4

信息安全 information security

信息安全是指信息网络的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，信息服务不中断。网络环境下的信息安全体系是保证信息安全的关键，包括计算机安全操作系统、各种安全协议、安全机制（数字签名，信息认证，数据加密等），直至安全系统，其中任何一个安全漏洞便可以威胁全局安全。信息安全服务至少应该包括支持信息网络安全服务的基本理论，以及基于新一代信息网络体系结构的网络安全服务体系结构。

3.1.5

交互 interaction

本规范中指医院信息平台与医院业务系统（临床服务系统、医疗管理系统、运营管理系统等）以及区域卫生信息平台之间的信息交换过程。一次特定的交互可能包含多个交易。

3.1.6

交易 transaction

本规范指角色对某个特定服务的调用。

3.2 缩略语

ACID: Atomicity Consistency Isolation Durability, 原子性、一致性、隔离性及持久性

ADSL：Asymmetric Digital Subscriber Line，非对称数字用户线路。

BPM：Business Process Manager，业务流程管理

CIFS：Common Internet File System,CIFS 是一种协议，它使程序可以访问远程Internet计算机上的文件并要求此计算机的服务

CLI：command-line interface，命令行界面

CPOE: Computerized Physician Order Entry 计算计化医嘱录入

CPU：Central Processing Unit，中央处理器

ECC：Error Correcting Code，错误检查和纠正技术

EDA：Event-driven Architecture，事件驱动架构

EHR：Electronic Health Record，电子健康档案、健康档案

EMR：Electronic Medical Record，电子病历

ESB：Enterprise Service Bus，企业服务总线

FC：Fiber Channel，光纤通道

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

FCSAN：光纤存储区域网络

FTP：File Transfer Protocol，文件传输协议

GUI：Graphical User Interface，图形用户界面

HTTP：HyperText Transfer Protocol，超文本传输协议，

I/O：Input/Output，即输入输出

IPMI：Intelligent Platform Management Interface，智能型平台管理接口

IPSAN：IP存储区域网络

iSCSI：Internet Small Computer System Interface,Internet小型计算机系统接口

Java EE：Java Enterprise Edition，Java企业版，1.5版以前称为J2EE

Java：Sun公司推出的面向对象的编程语言

KVM：Keyboard Video Mouse，即多计算机切换器

LED：Light Emitting Diode，发光二极管

NAS： Network Attached Storage，网络附加存储

NFS：Network File System,网络文件系统

ODS：Operational Data Store 操作数据存储

PCI：Peripheral Component Interconnect，计算机局部总线标准

PKI：Public Key Infrastructure，公开密钥体系

RAID：Redundant Array of Independent Disk,独立冗余磁盘阵列

RPO：Recovery Point Object,恢复点目标

RS232：RS-232是美国电子工业协会EIA（Electronic Industry Association）制定的一种串行物理接口标准。RS是英文“推荐标准”的缩写，232为标识号

RTO：Recovery Time Object,恢复时间目标

SAN：Storage Area Network，存储局域网络

SAS：Serial Attached SCSI，串行连接SCSI

SATA：Serial Advanced Technology Attachment,串行ATA

SMTP：Simple Mail Transfer Protocol，简单邮件传输协议

SNMP：Simple Network Management Protocol,简单网络管理协议

SOA：Service-oriented Architecure，面向服务的体系结构

SQL：StructuredQueryLanguage，结构化查询语言

SSD：Solid State Disk，固态硬盘

TCO：Total cost of ownership,总所有成本

TCP/IP：Transmission Control Protocol/Internet Protocol，传输控制协议/网际互联协议

Telnet：Telnet协议是TCP/IP协议族中的一种，是Internet远程登陆服务的标准协议和主要方式

VPN：Virtual Private Network，虚拟专用网络

4 软件技术总体要求

4.1 医院信息平台总体框架

医院信息平台总体框架主要包括基础设施、信息资源中心、医院信息平台服务、基于医院信息平台的应用、标准规范和信息安全，如下图所示。

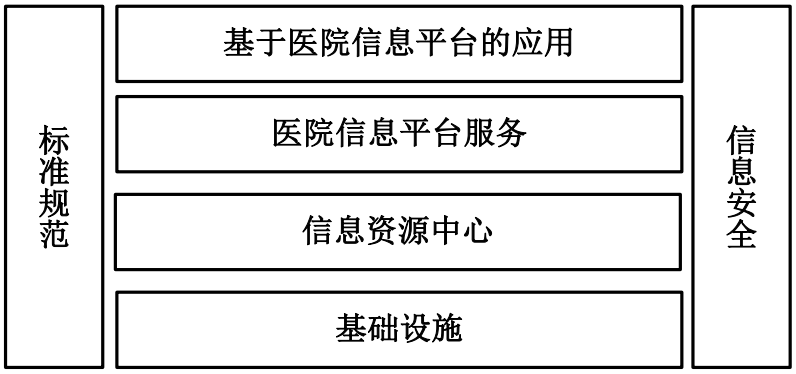

图1 医院信息平台总体框架

4.2 医院信息平台参考技术架构

本技术规范中的医院信息平台参考技术架构如下图所示：

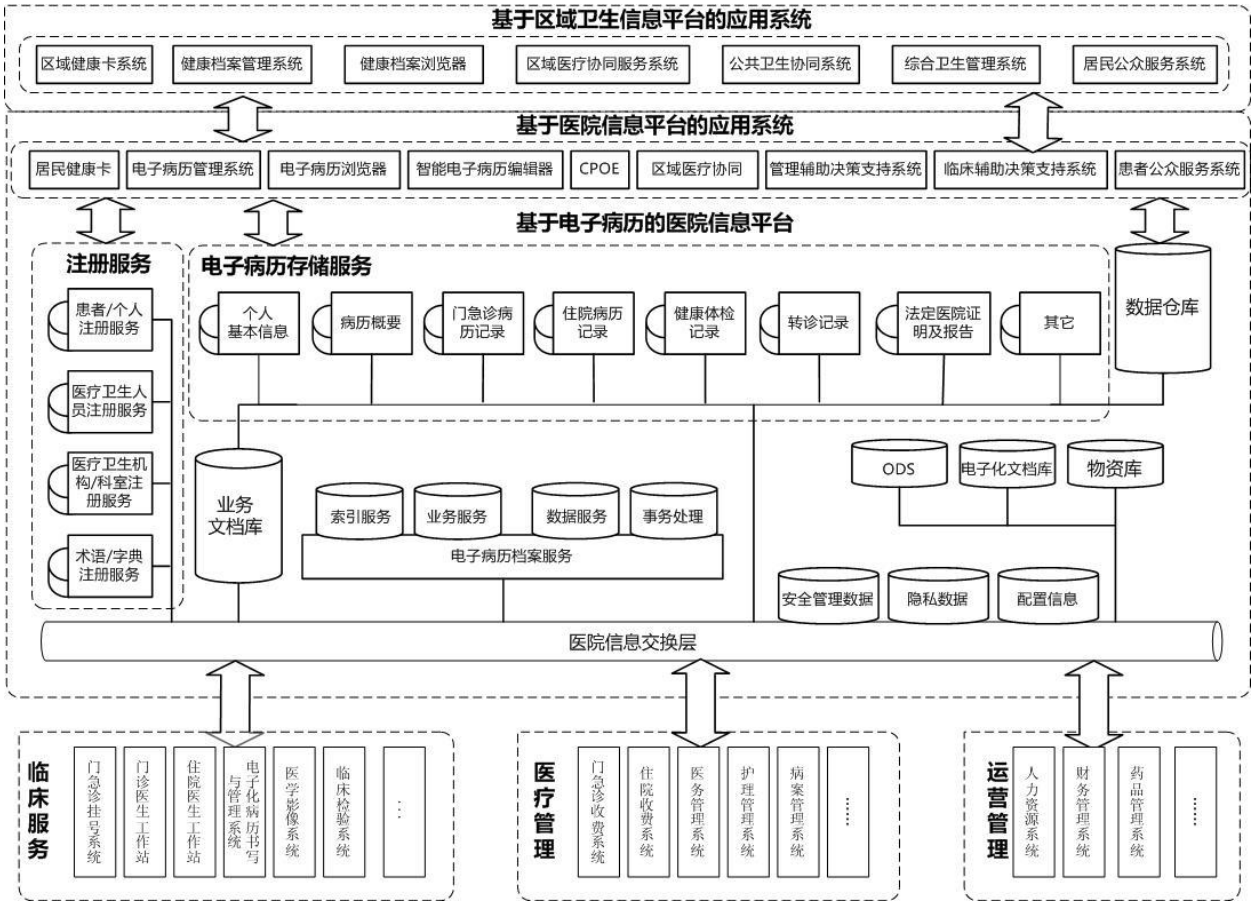

图2　医院信息平台参考技术架构

4.2.1　医院业务应用系统

医院业务应用是医院信息平台的基础，包括三大类业务系统：临床服务系统、医疗管理系统以及运营管理系统。

4.2.1.1　临床服务系统

主要包括门急诊挂号系统、门诊医生工作站、分诊管理系统、住院病人入出转系统、住院医生工作站、 住院护士工作站、 电子化病历书写与管理系统、 合理用药管理系统、临床检验系统、医学影像系统、超声/内镜/病理管理系统、手术麻醉管理系统、临床路径管理系统、输血管理系统、重症监护系统、心电管理系统、体检管理系统。

4.2.1.2　医疗管理系统

主要包括门急诊收费系统、住院收费系统、护理管理系统、医务管理系统、院感/传染病管理系统、科研教学管理系统、病案管理系统、医疗保险/新农合接口、职业病管理系统接口、食源性疾病上报系统接口。

4.2.1.3　运营管理系统

主要包括人力资源管理系统、财务管理系统、药品管理系统、设备材料管理系统、物资供应管理系统、预算管理系统。

4.2.2 医院信息交换层

医院信息平台信息交换层的主要任务以满足临床信息、医疗服务信息和医院管理信息的共享和协同应用为目标，采集相关业务数据，并对外部系统提供数据交换服务，包括与区域平台的数据交换。

4.2.3 医院信息平台资源层

医院信息平台信息资源层用于整个平台各类数据的存储、处理和管理，主要包括信息目录库、基础信息库、业务信息库、临床文档信息库 CDR、交换信息库、操作数据存储 ODS、数据仓库、对外服务信息库、智能化管理信息库。

4.2.4 医院信息平台应用层

基于医院信息平台的应用包括居民健康卡、电子病历管理系统、电子病历浏览器、智能电子病历编辑器、计算机化医嘱录入（CPOE）、区域医疗协同、管理辅助决策支持系统、临床辅助决策支持系统和患者公众服务系统等。

4.2.5 医院信息平台与区域卫生信息平台的互联互通

通过医院信息平台与区域卫生信息平台的对接，实现两级平台信息共享、业务协同。跨医院之间的信息共享、业务协同包括居民健康卡、区域诊疗信息共享、区域医疗协同、区域辅助医疗和区域医疗公众服务等应用。

4.3 医院信息平台软件架构要求

a) 医院信息平台软件架构应该基于面向服务架构的思想来构建；
b) 医院信息平台要求具有消息路由功能，可以具有业务流程管理（BPM）、可以支持医院自动化业务流程编排和人工参与的工作流；
c) 医院信息平台架构应支持基于事件驱动(EDA)的消息传输机制，支持服务的发布与订阅。

4.4 功能要求

a) 医院信息平台应支持医院临床业务系统的集成和整合,可具有支持业务流程编排的功能；
b) 医院信息平台应提供管理工具,能够管理所有业务系统集成节点,监控整个医院平台运行状态；
c) 医院信息平台应支持用户授权及认证,支持数据防篡改及隐私数据保密，支持业务流程的追踪与审计，支持日志的记录与查看，支持消息可靠性传递及消息追踪等；
d) 医院信息平台应提供二次开发环境，提供基础公共业务组件的封装，并提供相应的维护管理工具。

4.5 交互信息的要求

a) 交互信息应支持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；
b) 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。

4.6 集成能力的要求

为了最大限度地复用现有应用系统的业务功能，在选择SOA技术标准规范时，必须考虑现有业务功能封装对技术标准规范的支持能力；

a) 以 Web Service 技术作为 SOA 服务开发技术的首选技术，并要求遵循 WS-I Basic Profile 1.0 的有关指引；
b) 医院信息平台可以支持主流的卫生信息交换国际标准和规范；
c) 基于 Web Service 的服务的安全管理应遵循 Web Service 服务规范中 WS-Security 规范，其他形式的服务也必须提供安全保障。

5 平台基本功能要求

5.1 基础服务

5.1.1 基本要求

基础服务应包括对患者、医疗服务人员、医疗卫生机构（科室）、医疗卫生术语和字典的注册管理服务。平台应对这些实体提供唯一的标识。针对各类实体形成各类注册库（如患者注册库、医疗服务人员注册库、机构注册库、术语和字典注册库）。

5.1.2 个人注册服务

个人注册服务用于对前来医院就诊患者的基本信息进行管理。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，可以为医院信息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：

a) 具备新增个人注册功能；
b) 具备个人信息更新功能；
c) 具备个人身份失效功能；
d) 具备个人身份合并功能；
e) 具备个人信息查询功能。

5.1.3 医疗卫生人员注册服务

医疗卫生人员注册服务用于对医疗卫生机构内部所有医疗服务人员的基本信息进行注册和管理。医疗服务人员包括医生、护士、医技人员、药事人员等全部提供医疗卫生服务的医务人员。通过对医疗卫生人员基本信息、专业信息的管理，可以为医院信息平台上的各应用系统，提供完整、统一的医疗卫生人员信息。基本功能要求包括：

a) 具备新增医护人员注册功能；
b) 具备医护人员信息更新功能；
c) 具备医护人员身份失效功能；
d) 具备医护人员身份合并功能；
e) 具备医护人员信息查询功能。

5.1.4 医疗卫生机构（科室）注册

医疗卫生机构（科室）注册用于对医疗卫生机构（科室）的基本信息进行管理。通过对医疗卫生机构（科室）基本信息的统一管理，可以为医院信息平台上的各应用系统、患者提供完整、统一的医疗卫生机构（科室）信息。基本功能要求包括：

a) 具备新增医疗卫生机构（科室）注册功能；
b) 具备医疗卫生机构（科室）信息更新功能；
c) 具备医疗卫生机构（科室）停用功能；

d) 具备医疗卫生机构（科室）信息查询功能。

5.1.5 术语和字典注册

术语和字典注册用于从数据定义层次来解决各系统的互操作问题。术语和字典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问题。术语应由平台管理者进行注册、更新和维护；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、更新和维护。基本功能要求包括：

a) 具备术语和字典的批量导入导出功能；
b) 具备术语和字典的分类浏览功能；
c) 具备术语和字典的关系维护功能；
d) 具备术语和字典的版本管理功能；
e) 具备术语和字典的映射关系维护功能；
f) 具备向其他系统同步术语和字典功能。

5.2 电子病历整合服务

5.2.1 就诊服务

就诊服务用于对患者的就诊信息进行管理。医院信息平台可以实现患者在就诊过程中入院、转科、出院等各环节信息的保存，变更和信息共享。基本功能要求包括：

a) 具备就诊信息接收功能；
b) 具备就诊信息订阅功能；
c) 具备就诊信息发布功能；
d) 具备就诊信息查询功能。

5.2.2 医嘱交互服务

医嘱交互服务用于对患者的整个临床诊疗过程中的医嘱信息的管理。医院信息平台在医嘱处理过程中(如医嘱开立、医嘱执行、医嘱停止、医嘱取消)为平台上的各应用系统提供医嘱信息共享服务。基本功能要求包括：

a) 具备医嘱接收功能；
b) 具备医嘱订阅功能；
c) 具备医嘱发布功能；
d) 具备医嘱查询功能。

5.2.3 申请单服务

申请单服务是医院信息平台为接入平台的各系统提供申请单(输血申请单、手术申请单、检查申请单、检验申请单等)信息共享服务。基本功能要求包括：

a) 具备申请单接收功能；
b) 具备申请单订阅功能；
c) 具备申请单发布功能；
d) 具备申请单查询功能。

5.2.4 预约信息服务

预约信息服务是医院信息平台在预约处理过程中为平台上的临床系统提供医疗资源信息共享服务。基本功能要求包括：

a) 具备预约排班信息接收功能；
b) 具备预约排班信息查询功能；
c) 具备预约确认功能；
d) 具备预约查询功能。

5.2.5 结果信息服务

结果信息服务是医院信息平台为接入平台的各系统提供观察结果、业务活动记录(检查报告、检验报告、电子病历文档等) 信息共享服务。基本功能要求包括：

a) 具备结果信息接收功能；
b) 具备结果信息订阅功能；
c) 具备结果信息发布功能；
d) 具备结果信息查询功能。

5.3 电子病历档案服务

5.3.1 索引服务

索引服务用于将所有关于个人的诊疗信息事件，包括个人的就诊时间、科室、接受的医疗服务、产生的业务活动记录的索引信息保存到文档注册库中。通过索引服务可以从基本业务系统查看个人的诊疗事件信息，以及事件信息所涉及的文档目录及摘要信息。基本功能要求包括：

a) 具备静态文档注册功能；
b) 支持根据医疗事件或个人信息查询相关医疗静态文档索引的功能。

5.3.2 存储服务

用于接收电子病历文档,并将文档存储到文档存储库中，同时对文档的版本及生命周期管理，它还提供文档注册服务。基本功能包括：

a) 具备接收文档功能；
b) 具备向文档索引库注册文档功能；
c) 具备向文档使用者提供文档功能。

5.4 医院信息平台与区域卫生信息平台的交互服务

5.4.1 基本要求

医院内各信息系统应统一通过医院信息平台实现与区域卫生信息平台的交互,进而实现与外部机构的信息共享与业务协同。与区域卫生信息平台的交互规范应满足WS XXX-2012 基于居民健康档案的区域卫生信息平台技术规范的要求。医院信息平台应实现如下针对区域卫生信息平台的服务调用接口。

5.4.2 个人注册服务调用

a) 具备调用区域卫生信息平台的个人注册服务功能；
b) 具备调用区域卫生信息平台的个人 ID 查询服务功能；
c) 具备调用区域卫生信息平台的个人基本信息查询服务功能。

5.4.3 医疗卫生人员注册服务调用

具备调用区域卫生信息平台的医疗卫生人员注册服务功能。

5.4.4 医疗卫生机构(科室)注册服务调用

具备调用区域卫生信息平台的医疗卫生机构注册服务功能。

5.4.5 医疗卫生术语注册服务调用

具备调用区域卫生信息平台的医疗卫生术语注册服务功能。

5.4.6 健康档案调阅服务调用

a) 具备调用区域卫生信息平台的调阅预判服务功能；
b) 具备调用区域卫生信息平台的调阅展现服务功能；
c) 具备调用区域卫生信息平台的调阅目录服务功能；
d) 具备调用区域卫生信息平台的摘要调阅服务功能。

5.4.7 病历文档上传服务调用

a) 具备调用区域卫生信息平台的文档上传服务功能；
b) 病历文档的范围参见 WS XXX-2012 基于居民健康档案的区域卫生信息平台技术规范 10.3.1。

5.4.8 病历数据查询服务调用

a) 具备调用区域卫生信息平台的病历数据查询服务功能；
b) 病历数据的范围参见 WS XXX-2012 基于居民健康档案的区域卫生信息平台技术规范 10.3.1。

5.5 信息安全及隐私服务

5.5.1 用户管理及授权服务

医院信息平台应为各应用系统提供统一的用户授权管理服务。 基本功能要求包括：
a) 具备用户角色创建功能；
b) 具备用户授权功能；
c) 具备访问规则定制功能，并按规则访问数据的功能；
d) 具备记录用户权限操作日志功能。

5.5.2 信息安全服务

医院信息平台应提供统一的信息安全服务，用户在信息交互时平台通过认证等方式保证信息安全。功能要求参见9.3.5.2 信息安全。

5.5.3 隐私保护服务

医院信息平台应提供患者隐私数据保护服务。功能要求参见9.3.5.3 隐私保护。

5.5.4 审计追踪服务

医院信息平台应提供记录所有信息访问或信息更新操作日志，并提供数据的审计及操作追踪服务。功能要求参见 9.3.5.4 审计追踪。

6 信息资源规范

6.1 基础信息库

6.1.1 基本要求

医院信息平台的基础信息库包括患者基本信息库、医疗卫生服务人员信息库、医疗卫生机构（科室）信息、术语和字典信息库。基础信息库由医院信息平台的注册服务产生，并为这些实体提供唯一的标识。

6.1.2 患者基本信息库

患者基本信息库的主要内容可以按照卫生部《电子病历基本架构与数据标准（试行）》的规定，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 医疗卫生服务人员信息库

医疗卫生服务人员信息库的主要内容可以按照卫生部《电子病历基本架构与数据标准（试行）》的规定，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）信息库的主要内容可以按照卫生部《电子病历基本架构与数据标准（试行）》的规定，应包括该标准的H.08 卫生服务机构数据组。

6.1.5 术语和字典库

基于电子病历的医院信息平台的术语和字典库，应支持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、WS XXX-2012 电子病历基本数据集、《电子病历基本架构与数据标准（试行）》等规范。还应支持GB/T 2261.1-2003 个人基本信息分类与代码 第1部分 人的性别代码、GB/T 2261.2-2003 个人基本信息与分类代码婚姻状况代码、GB/T 2261.4-2003 个人基本信息分类与代码 第4部分 从业状况(个人身份)代码、GB/T 4658-1984 文化程度代码、GB 3304-1991 中国各民族名称的罗马字母拼写法和代码、疾病分类与代码（修订版）卫办综发［2011］166 号、ICD-9-CM-3 手术与操作、GB/T15657—1995 中医病证分类与代码、GB/T16751.3-1997 中医临床诊疗术语治则治法部分、GB/T 2659-2000 世界各国和地区名称代码。

6.2 临床文档库

6.2.1 文档存储库

文档存储库应负责将基于活动的，进行过标准化转换的临床文档，以明晰、安全和持久的方式进行存储。文档存储库内容应符合卫生部《电子病历基本架构与数据标准（试行）》的规定。

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作出响应。

6.2.2 文档注册库

文档注册库应提供文档存储库的临床文档索引信息，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 交互规范

7.1 基础服务

7.1.1 个人注册服务

个人注册服务中包括三个角色：个人注册服务、个人身份源和个人身份使用者。个人注册服务向个人身份源和个人身份使用者提供服务。

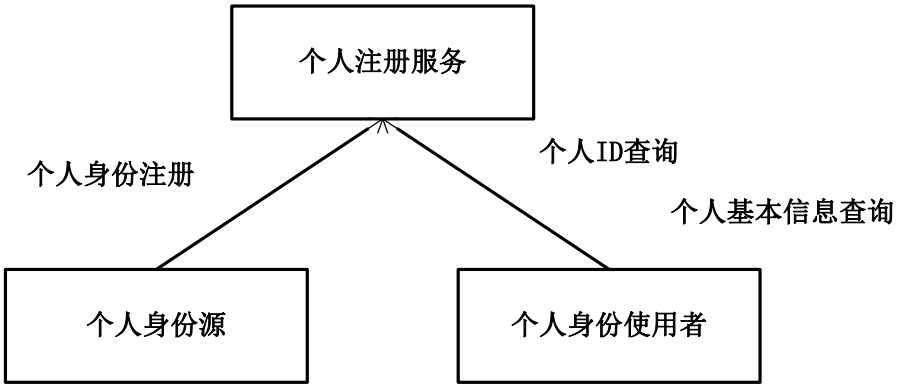

图3 个人注册角色交易图

个人注册服务组件应提供个人身份注册服务、个人ID查询服务和个人基本信息查询服务。

7.1.1.1 个人身份注册服务

在个人身份建立、修改或合并时可以使用本服务注册个人信息。

7.1.1.1.1 角色和交易

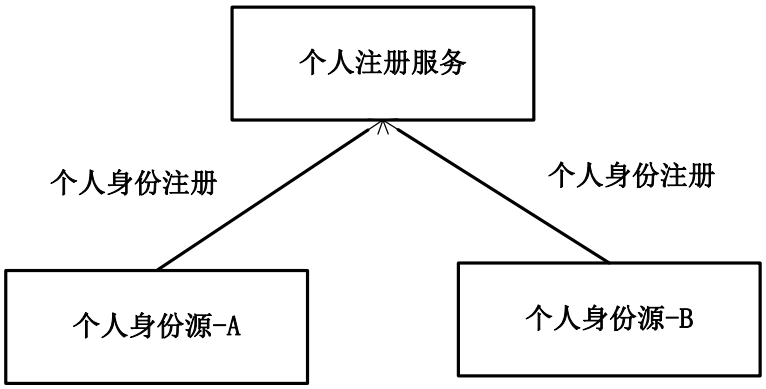

图4 个人注册角色交易图

7.1.1.1.2 角色的选择

表1 个人注册角色

角色	交易	选择
个人身份源	个人身份提交	必须（R）
个人注册服务	个人身份提交	必须（R）

7.1.1.1.3　交易流程

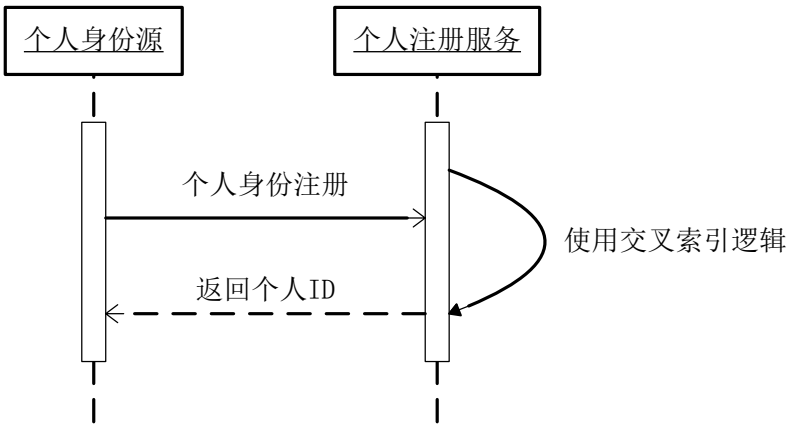

图5　个人身份注册服务时序图

- 个人身份源向个人注册服务提交个人身份信息；
- 个人注册服务对个人身份源提交的个人信息建立交叉索引；
- 个人注册服务校验数据并进行存储。

7.1.1.2　个人基本信息查询服务

7.1.1.2.1　角色和交易

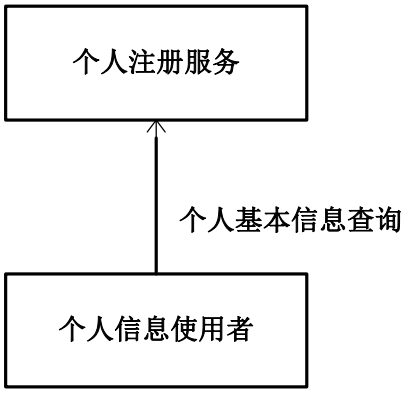

图6　个人基本信息查询角色交易图

7.1.1.2.2　角色的选择

表2　个人基本信息查询角色

角色	交易	选择
个人基本信息使用者	个人基本信息查询	必须（R）
个人注册服务	个人基本信息查询	必须（R）

7.1.1.2.3　交易流程

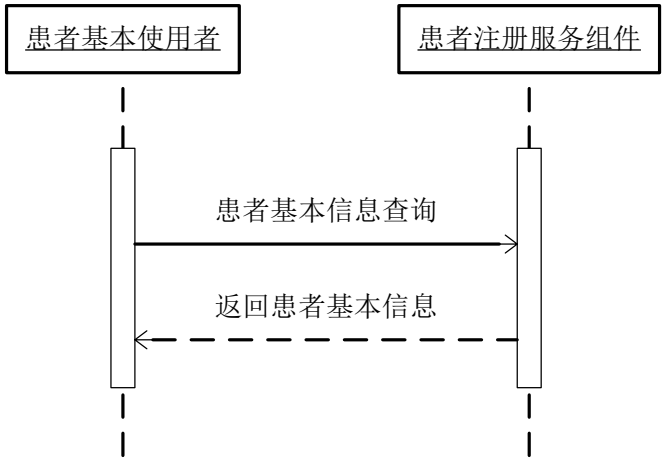

图7　个人基本信息查询服务时序图

- 个人基本信息使用者向个人注册服务提交个人基本信息查询；
- 个人注册服务返回个人基本信息。

7.1.2　医疗卫生人员注册

7.1.2.1　角色和交易

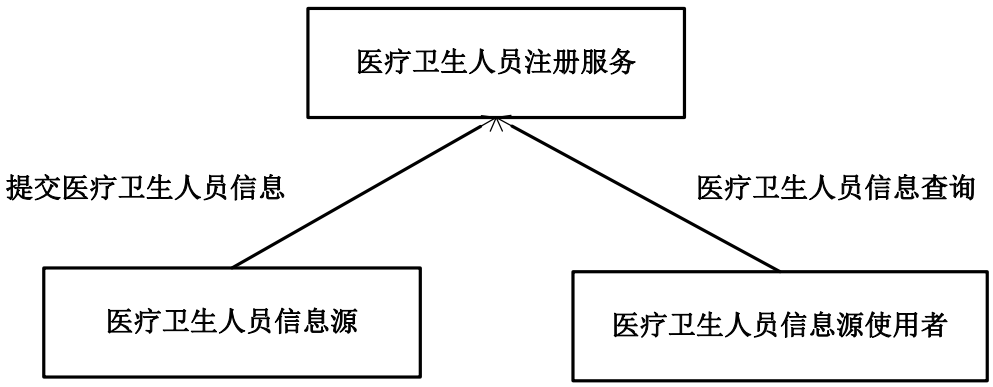

图8　医疗卫生人员注册角色交易图

7.1.2.2　角色的选择

表3　医疗卫生人员注册角色

角色	交易	选择
医疗卫生人员信息源	医疗卫生人员注册	必须（R）
医疗卫生人员信息使用者	医疗卫生人员信息查询	必须（R）
医疗卫生人员注册服务	医疗卫生人员注册	必须（R）
医疗卫生人员注册服务	医疗卫生人员信息查询	必须（R）

7.1.2.3 交易流程

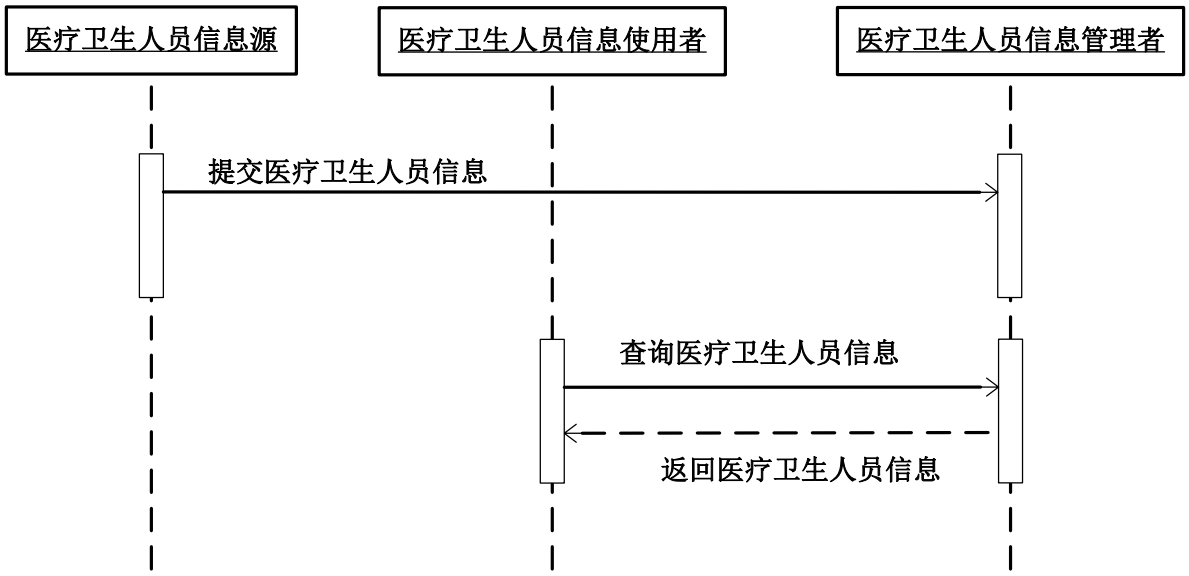

图9 医疗人员注册服务时序图

- 医院内科室系统（如医院 HIS 系统）作为医疗卫生人员信息源，向医院信息平台中医疗人卫生员注册服务提交本科室的医疗卫生人员信息；
- 医院内科室系统（如医生工作站）在某个跨科室业务中，查询相关医疗卫生人员的信息。

7.1.3 医疗卫生机构(科室)注册

7.1.3.1 角色和交易

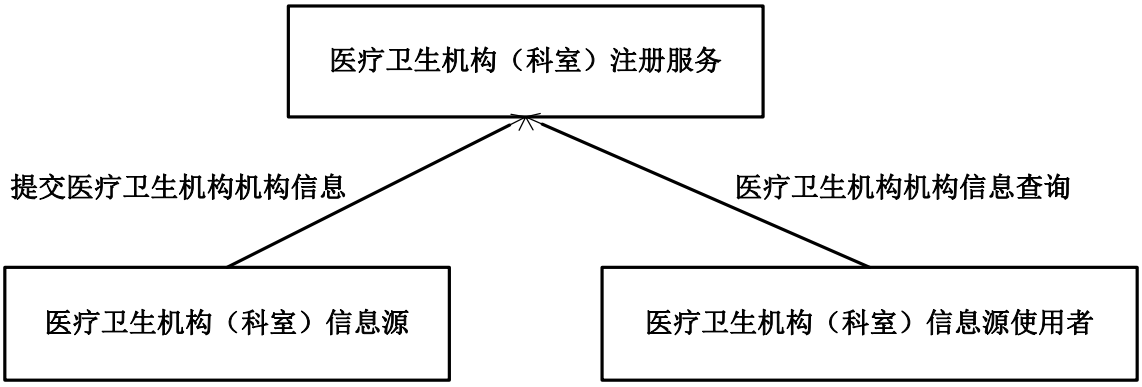

图10　医疗卫生机构（科室）注册角色交易图

7.1.3.2　角色的选择

表4　医疗卫生机构（科室）注册角色

角色	交易	选择
医疗卫生机构（科室）信息源	医疗卫生机构（科室）注册	必须（R）
医疗卫生机构（科室）信息使用者	医疗卫生机构（科室）查询	必须（R）
医疗卫生机构（科室）注册服务	医疗卫生机构（科室）注册	必须（R）
	医疗卫生机构（科室）信息查询	必须（R）

7.1.3.3　交易流程

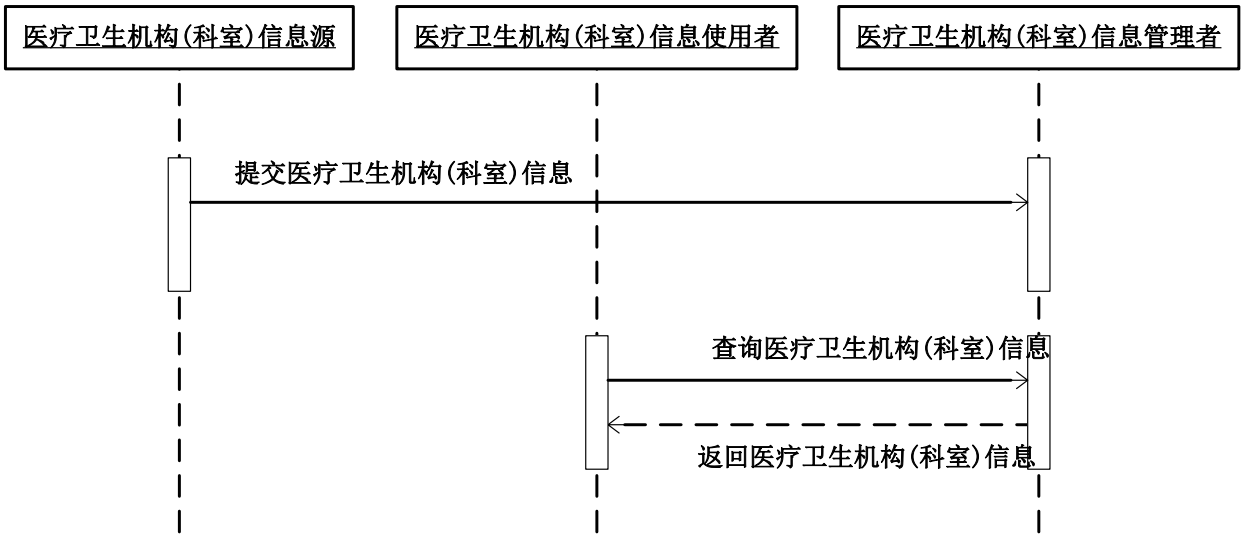

图11　医疗卫生机构（科室）注册服务时序图

- 医院内医院管理系统作为机构信息源，向医院信息平台中机构注册服务提交医疗卫生机构信息；

- 医院内科室系统（如医生工作站）在某个跨科室的业务中，查询医疗卫生机构（科室）的信息。

7.1.4 术语和字典注册

7.1.4.1 术语和字典注册服务

7.1.4.1.1 角色和交易

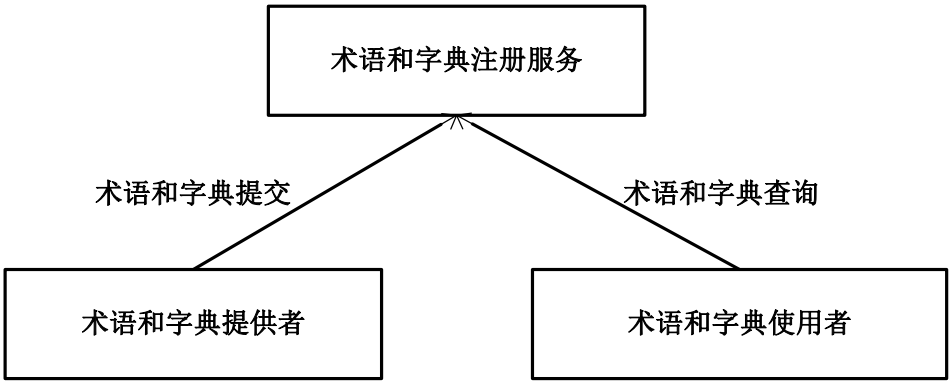

图12 术语和字典注册角色交易图

术语和字典注册活动主要有三角色参与，术语和字典注册服务与术语和字典提供者、术语和字典使用者。

7.1.4.1.2 角色的选择

表5 术语和字典注册角色

角色	交易	选择
术语和字典提供者	术语和字典提交	必须（R）
术语和字典使用者	术语和字典查询	必须（R）
术语和字典注册服务	术语和字典提交	必须（R）
	术语和字典查询	必须（R）

7.1.4.1.3 交易流程

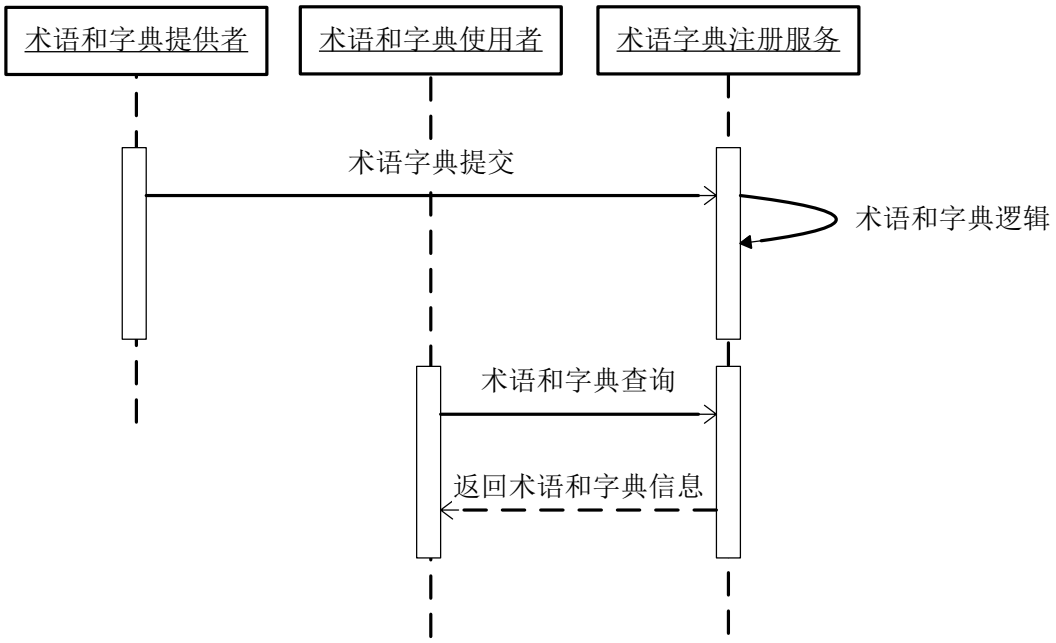

图13　术语和字典注册服务时序图

- 术语和字典提供者提交术语字典到术语和字典注册服务；
- 术语和字典使用者提交术语和字典查询请求到术语和字典注册服务；
- 术语和字典注册服务校验数据并进行存储。

7.1.4.2　术语和字典映射服务

7.1.4.2.1　角色和交易

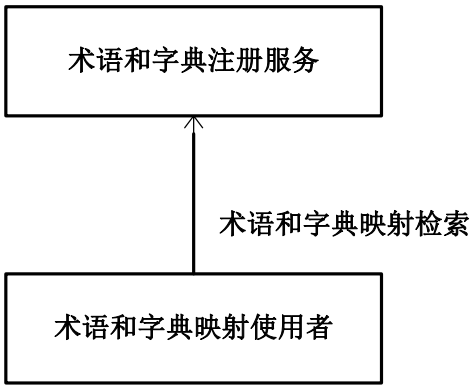

图14　术语和字典映射角色交易图

术语和字典映射活动主要有两类角色参与，术语和字典映射服务和术语和字典映射使用者。由术语和字典映射使用者向术语和字典映射服务组件提交术语和字典映射匹配检索请求，术语和字典注册服务组件返回相应的目标代码检索结果。

7.1.4.2.2　角色的选择

表6　术语和字典映射角色

角色	交易	选择
术语和字典映射使用者	术语和字典映射检索	必须（R）
术语和字典注册服务	术语和字典映射检索	必须（R）

7.1.4.2.3　交易流程

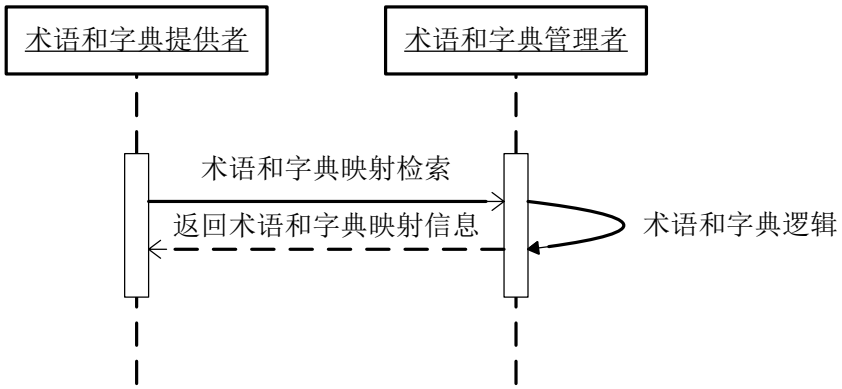

图15　术语和字典映射服务时序图

- 术语和字典映射使用者提交源代码检索请求；
- 术语和字典注册服务在术语和字典库中检索目标代码，并将结果返回给术语和字典映射使用者。

7.2　电子病历整合服务

7.2.1　就诊信息服务

7.2.1.1　就诊信息接收服务

7.2.1.1.1　角色和交易

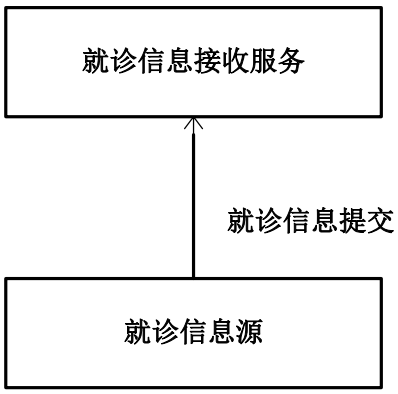

图16　就诊信息接收角色交易图

就诊信息接收活动主要有两类角色参与，平台就诊信息接收服务和就诊信息源。由就诊信息源向就诊信息接收服务提交就诊信息。

7.2.1.1.2　角色的选择

表7　就诊信息接收角色

角色	交易	选择
就诊信息源	就诊信息提交	必须（R）
就诊信息接收服务	就诊信息提交	必须（R）

7.2.1.1.3　交易流程

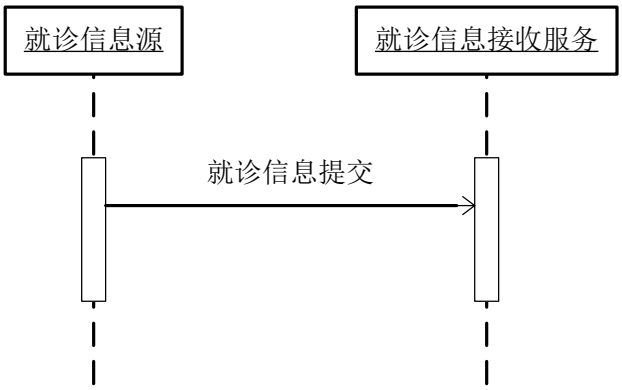

图17　就诊信息接收服务时序图

- 就诊信息源提交就诊信息到就诊信息接收服务；
- 就诊信息接收服务校验数据并进行存储。

7.2.1.2　就诊信息订阅服务

7.2.1.2.1　角色和交易

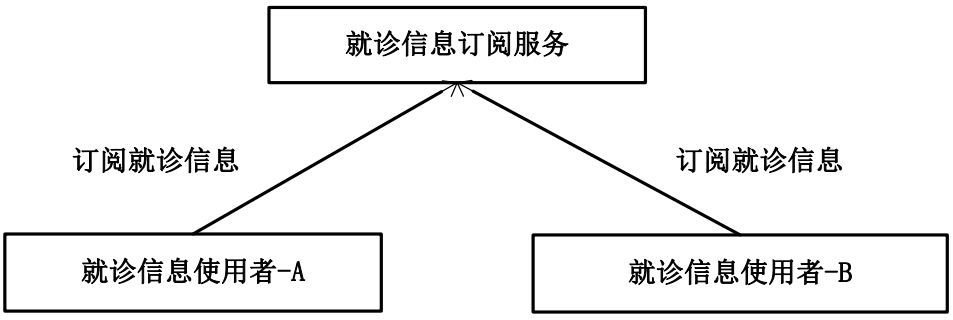

图18　就诊信息订阅角色交易图

7.2.1.2.2　角色的选择

表8　就诊信息订阅角色

角色	交易	选择
就诊信息使用者	订阅就诊信息	必须（R）
就诊信息订阅服务	订阅就诊信息	必须（R）

7.2.1.2.3 交易流程

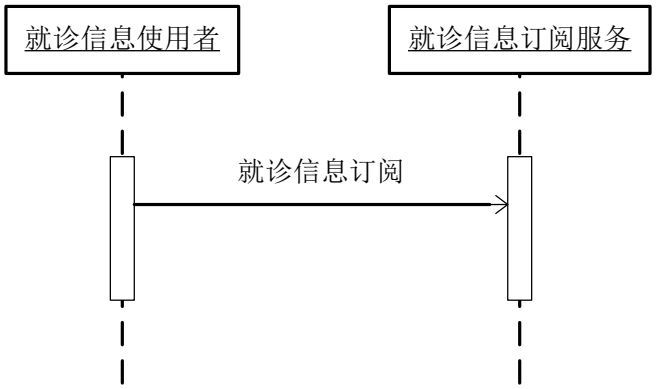

图19 就诊信息订阅服务时序图

- 就诊信息使用者订阅就诊信息到就诊信息订阅服务；
- 就诊信息订阅服务校验数据并进行存储。

7.2.1.3 就诊信息发布服务

7.2.1.3.1 角色和交易

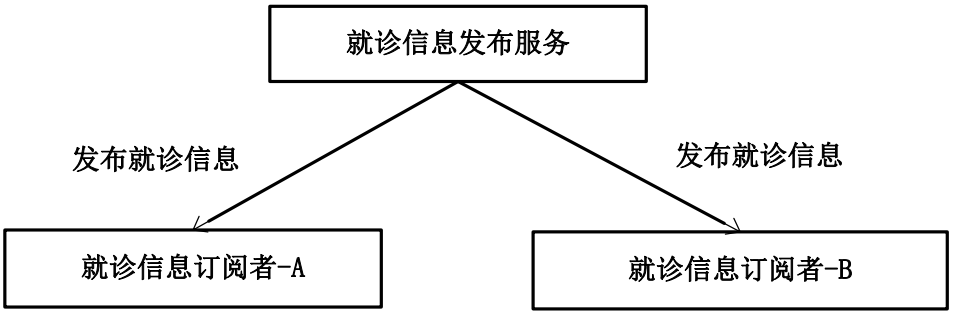

图20 就诊信息发布角色交易图

7.2.1.3.2 角色的选择

表9 就诊信息发布角色

角色	交易	选择
就诊信息订阅者	发布就诊信息	必须（R）
就诊信息发布服务	发布就诊信息	必须（R）

7.2.1.3.3 交易流程

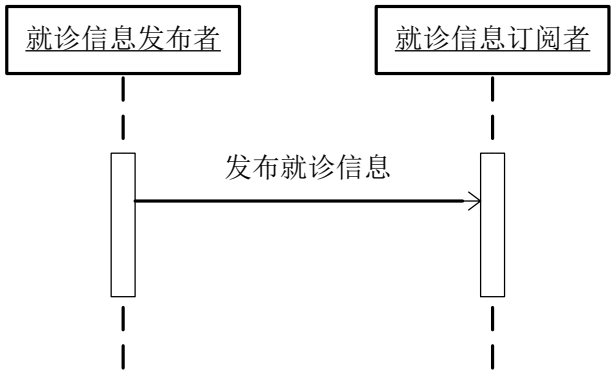

图21 就诊信息发布服务时序图

- 就诊信息发布者将就诊信息发布到就诊信息订阅者；
- 就诊信息订阅者接收就诊信息。

7.2.1.4 就诊查询服务

7.2.1.4.1 角色和交易

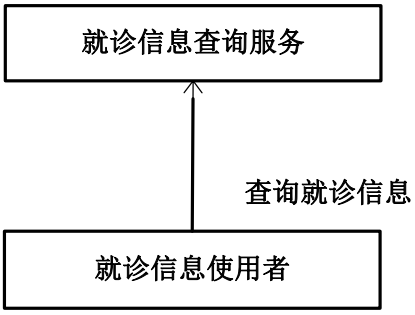

图22 就诊信息查询角色交易图

7.2.1.4.2 角色的选择

表10 就诊信息查询角色

角色	交易	选择
就诊信息使用者	查询就诊信息	必须（R）
就诊信息查询服务	查询就诊信息	必须（R）

7.2.1.4.3 交易流程

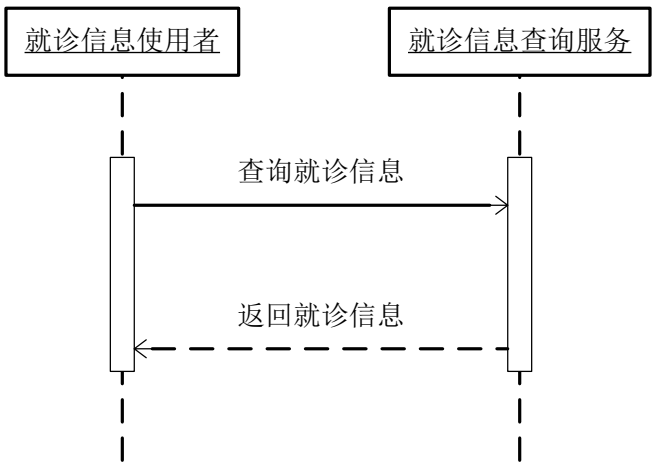

图23　就诊信息查询服务时序图

- 就诊信息使用者将查询就诊信息的请求提交到就诊信息查询服务；
- 就诊信息查询服务将查询结果返回给就诊信息使用者。

7.2.2　医嘱信息服务

7.2.2.1　医嘱接收服务

7.2.2.1.1　角色和交易

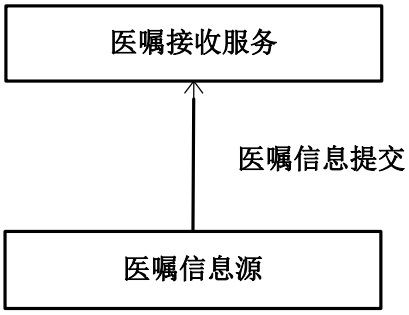

图24　医嘱接收服务角色交易图

医嘱信息接收活动主要有两类角色参与，医嘱信息接收服务和医嘱信息源。由医嘱信息源向医嘱信息接收服务提交医嘱信息。

7.2.2.1.2　角色的选择

表11　医嘱接收角色

角色	交易	选择
医嘱接收服务	医嘱信息提交	必须（R）

医嘱信息源	医嘱信息提交	必须（R）

7.2.2.1.3 交易流程

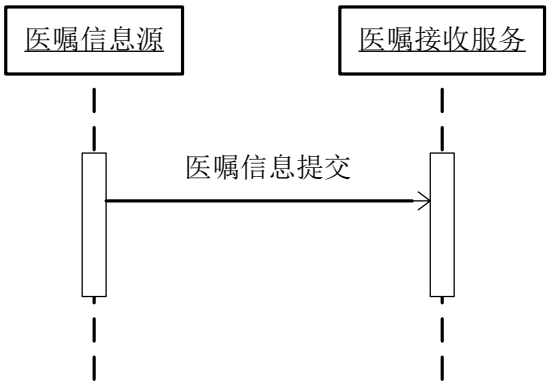

图25 医嘱接收服务时序图

- 医嘱信息源提交医嘱信息到医嘱接收服务；
- 医嘱接收服务校验数据并进行存储。

7.2.2.2 医嘱订阅服务

7.2.2.2.1 角色和交易

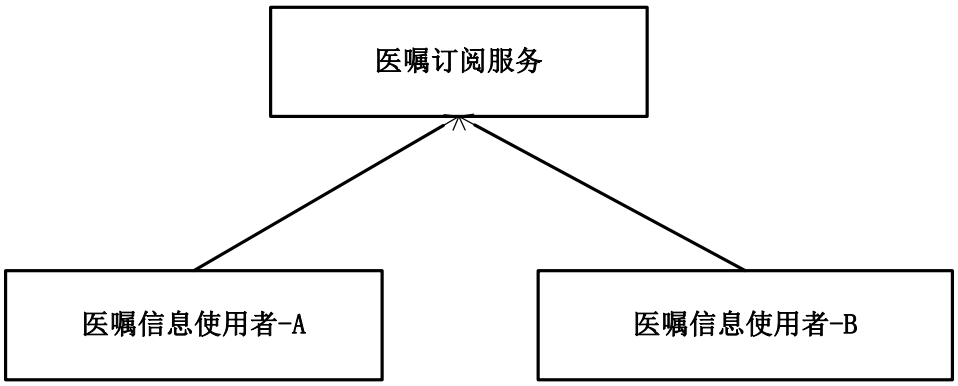

图26 医嘱订阅服务角色交易图

7.2.2.2.2 角色的选择

表12 医嘱订阅角色

角色	交易	选择
医嘱订阅服务	医嘱信息订阅	必须（R）

医嘱信息使用者	医嘱信息订阅	必须（R）

7.2.2.2.3 交易流程

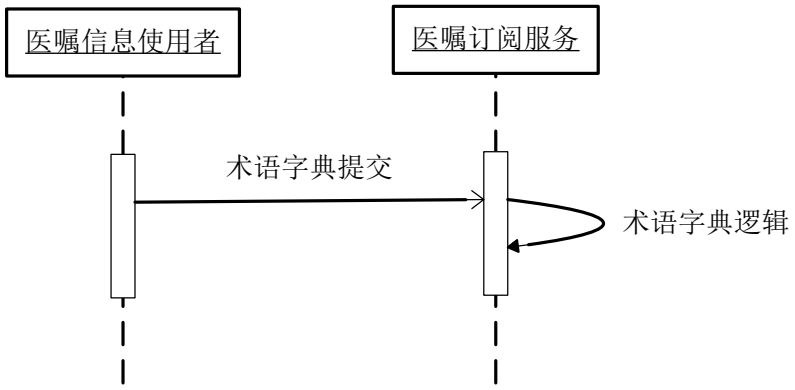

图27 医嘱订阅服务时序图

- 医嘱信息使用者订阅医嘱信息到医嘱信息订阅服务；
- 医嘱订阅服务校验数据并进行存储。

7.2.2.3 医嘱发布服务

7.2.2.3.1 角色和交易

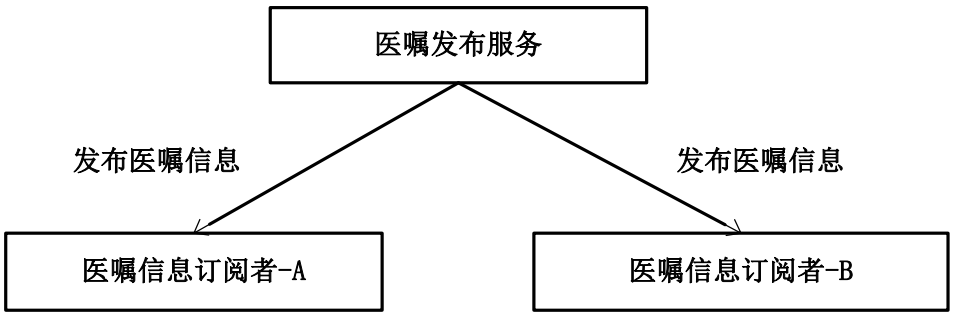

图28 医嘱发布服务角色交易图

7.2.2.3.2 角色的选择

表13 医嘱发布角色

角色	交易	选择
医嘱发布服务	医嘱信息发布	必须（R）
医嘱信息订阅者	医嘱信息发布	必须（R）

7.2.2.3.3 交易流程

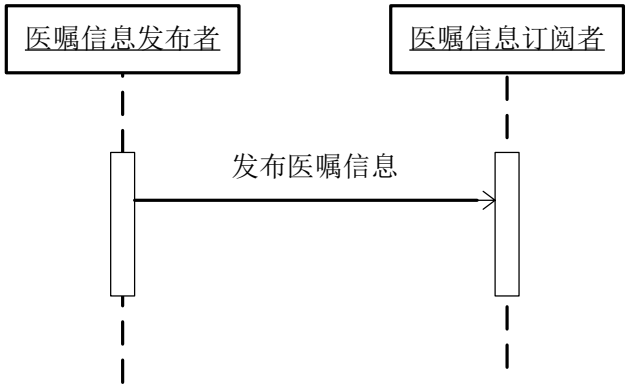

图29 医嘱发布服务时序图

- 医嘱信息发布者将医嘱信息发布给医嘱信息订阅者；
- 医嘱信息订阅者接收医嘱信息。

7.2.2.4 医嘱查询服务

7.2.2.4.1 角色和交易

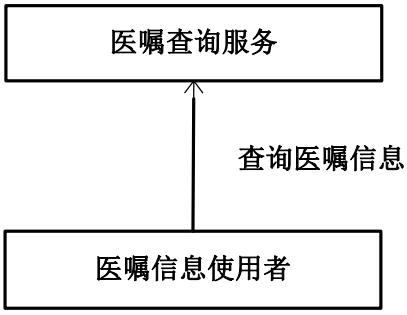

图30 医嘱查询服务角色交易图

7.2.2.4.2 角色的选择

表14 医嘱查询角色

角色	交易	选择
医嘱查询服务	查询医嘱信息	必须（R）
医嘱信息使用者	查询医嘱信息	必须（R）

7.2.2.4.3 交易流程

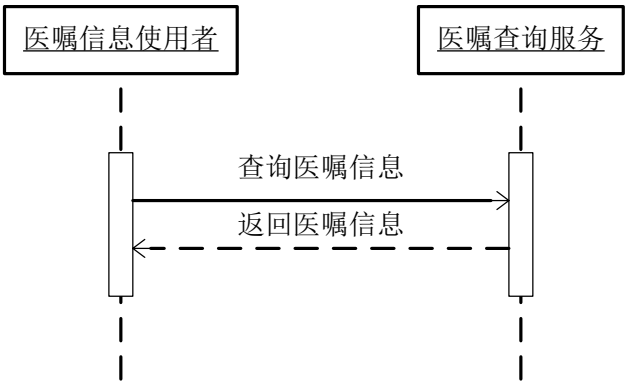

图31　医嘱查询服务时序图

- 医嘱信息使用者将查询医嘱信息请求提交到医嘱信息查询服务；
- 医嘱信息查询服务将查询结果返回给医嘱信息使用者。

7.2.3　申请单信息服务

7.2.3.1　申请单接收服务

7.2.3.1.1　角色和交易

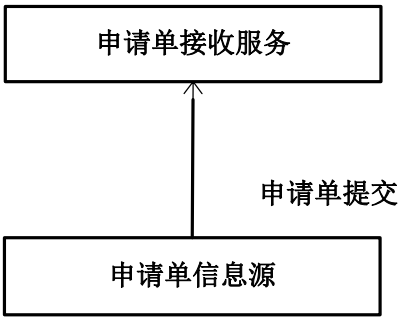

图32　申请单接收服务角色交易图

申请单信息接收活动主要有两类角色参与，申请单信息接收服务和申请单信息源。由申请单信息源向申请单信息接收服务提交申请单信息。

7.2.3.1.2　角色的选择

表15　申请单信息接收角色

角色	交易	选择
申请单信息接收服务	申请单信息提交	必须（R）

申请单信息源	申请单信息提交	必须（R）

7.2.3.1.3 交易流程

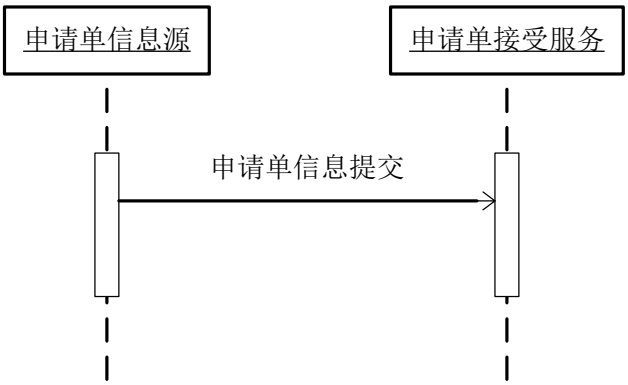

图33 申请单接收服务时序图

- 申请单信息源提交申请单信息到申请单接收服务；
- 申请单接收服务校验数据并进行存储。

7.2.3.2 申请单订阅服务

7.2.3.2.1 角色和交易

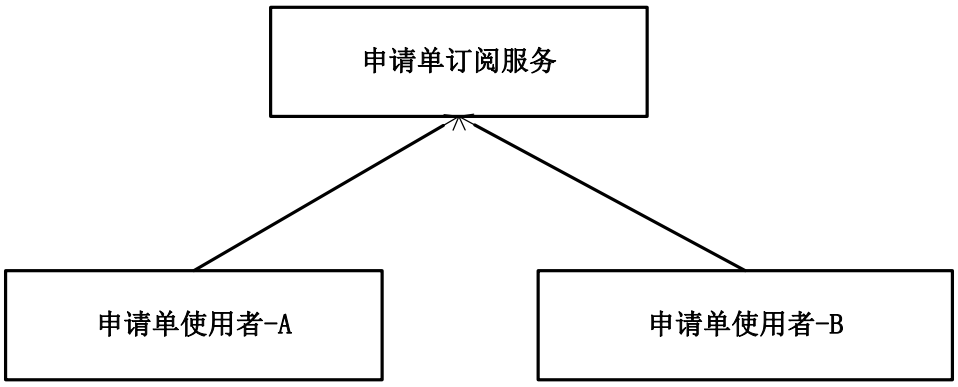

图34 申请单订阅服务角色交易图

7.2.3.2.2 角色的选择

表16 申请单订阅角色

角色	交易	选择
申请单订阅服务	订阅申请单信息	必须（R）

申请单使用者	订阅申请单信息	必须（R）

7.2.3.2.3 交易流程

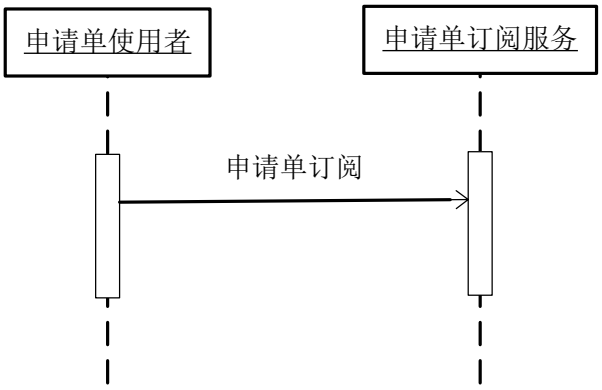

图35 申请单订阅服务时序图

- 申请单使用者订阅申请单信息到申请单订阅服务；
- 申请单订阅服务校验数据并进行存储。

7.2.3.3 申请单发布服务

7.2.3.3.1 角色和交易

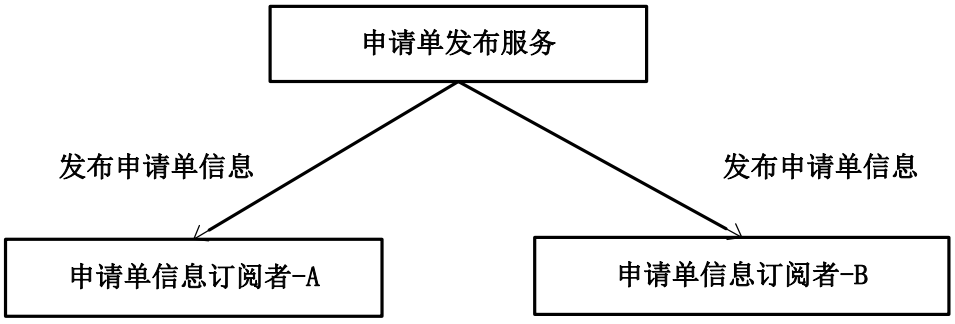

图36 申请单发布服务角色交易图

7.2.3.3.2 角色的选择

表17 申请单发布角色

角色	交易	选择
申请单发布服务	申请单信息发布	必须（R）
申请单信息订阅者	申请单信息发布	必须（R）

7.2.3.3.3 交易流程

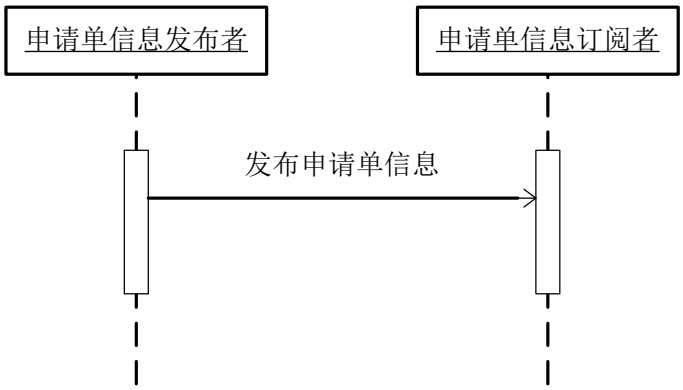

图37 申请单发布服务时序图

- 申请单信息发布者将申请单信息发布给申请单信息订阅者；
- 申请单信息订阅者接收申请单信息。

7.2.3.4 申请单查询服务

7.2.3.4.1 角色和交易

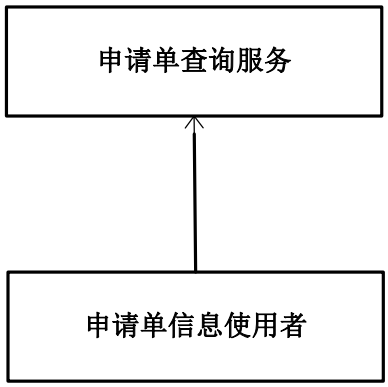

图38 申请单查询服务角色交易图

7.2.3.4.2 角色的选择

表18 申请单信息查询角色

角色	交易	选择
申请单信息查询服务	查询申请单信息	必须（R）

申请单信息使用者	查询申请单信息	必须（R）

7.2.3.4.3　交易流程

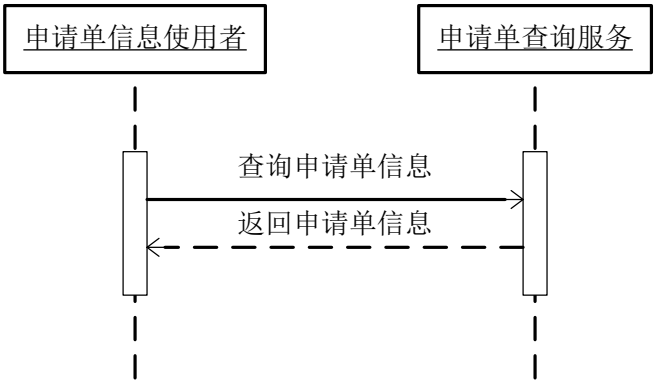

图39　申请单查询服务时序图

- 申请单信息使用者将查询申请单信息请求提交到申请单信息查询服务；
- 申请单信息查询服务将查询结果返回给申请单信息使用者。

7.2.4　预约信息服务

7.2.4.1　预约排班信息接收服务

7.2.4.1.1　角色和交易

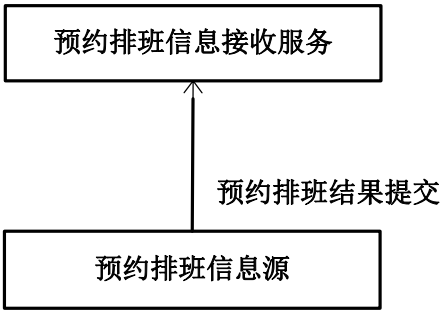

图40　预约排班信息接收服务角色交易图

预约排班信息接收活动主要有两类角色参与，预约排班信息接收服务和预约排班信息源。由预约排班信息源向预约排班信息接收服务提交预约排班信息。

7.2.4.1.2　角色的选择

表19　预约排班信息接收角色

角色	交易	选择
预约排班信息接收服务	预约排班信息提交	必须（R）
预约排班信息源	预约排班信息提交	必须（R）

7.2.4.1.3 交易流程

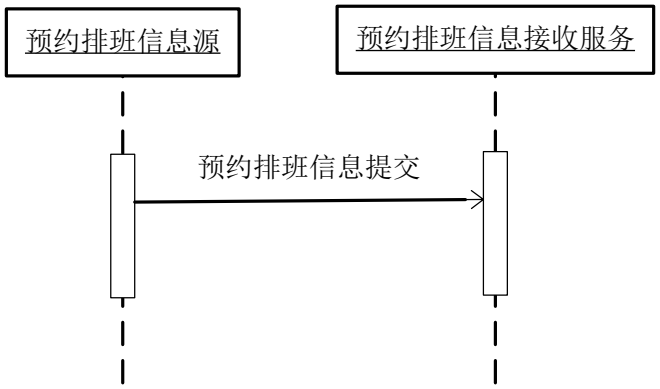

图41 预约排班信息服务时序图

- 预约排班信息源提交预约排班信息到预约排班信息接收服务；
- 预约排班信息接收服务校验数据并进行存储。

7.2.4.2 预约排班信息查询服务

7.2.4.2.1 角色和交易

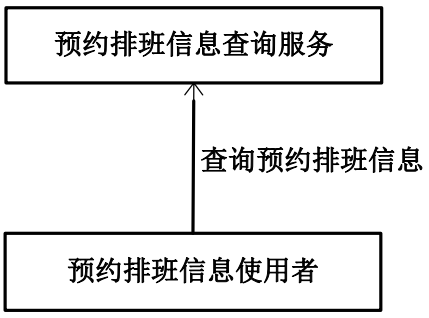

图42 预约排班查询服务角色交易图

7.2.4.2.2 角色的选择

表20 预约排班查询服务角色

角色	交易	选择

预约排班信息查询服务	查询预约排班信息	必须（R）
预约排班信息使用者	查询预约排班信息	必须（R）

7.2.4.2.3 交易流程

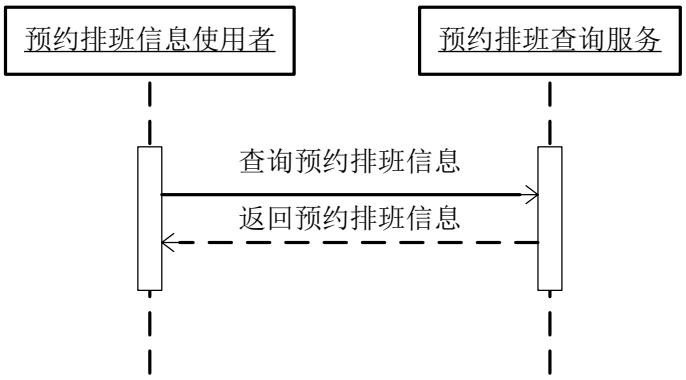

图43 预约排班查询服务交易时序图

- 预约排班信息使用者将查询预约排班信息请求提交到预约排班信息查询服务；
- 预约排班信息查询服务将查询结果返回给预约排班信息使用者。

7.2.4.3 预约确认服务

7.2.4.3.1 角色和交易

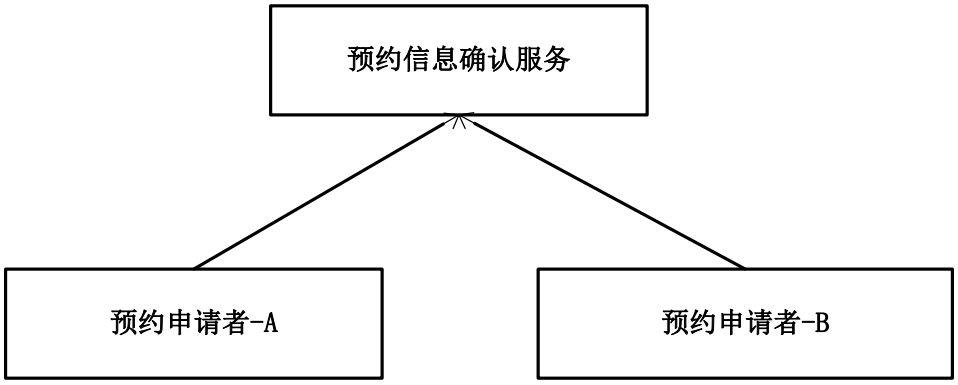

图44 预约确认服务角色交易图

7.2.4.3.2 角色的选择

表21 预约确认角色

角色	交易	选择
预约申请者	预约确认信息	必须（R）

预约信息确认服务	预约确认信息	必须（R）

7.2.4.3.3 交易流程

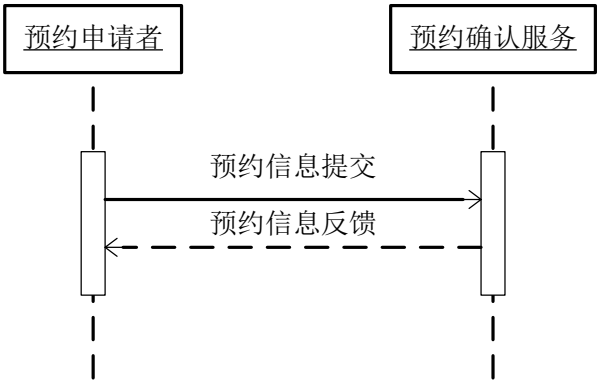

图45 预约信息确认服务时序图

- 预约申请者提交申请信息到预约确认服务；
- 预约确认服务校验数据并进行存储和反馈信息。

7.2.4.4 预约查询服务

7.2.4.4.1 角色和交易

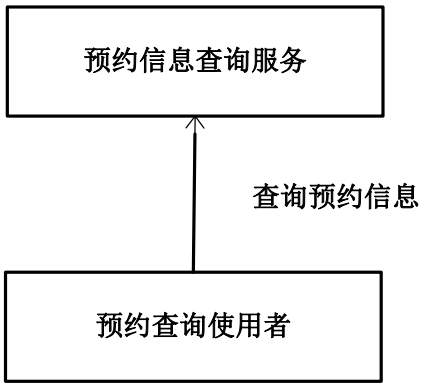

图46 预约查询服务角色交易图

7.2.4.4.2 角色的选择

表22 预约查询角色

角色	交易	选择

预约信息查询服务	查询预约信息	必须（R）
预约查询使用者	查询预约信息	必须（R）

7.2.4.4.3 交易流程

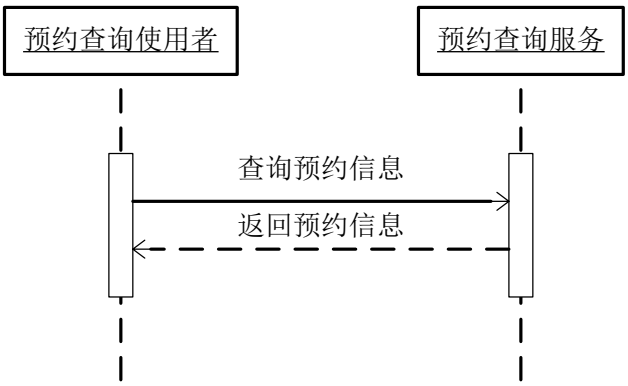

图47 预约查询服务时序图

- 预约信息使用者将查询预约信息请求提交到预约信息查询服务；
- 预约信息查询服务将查询结果返回给预约信息使用者。

7.2.5 结果信息服务

7.2.5.1 结果信息接收服务

7.2.5.1.1 角色和交易

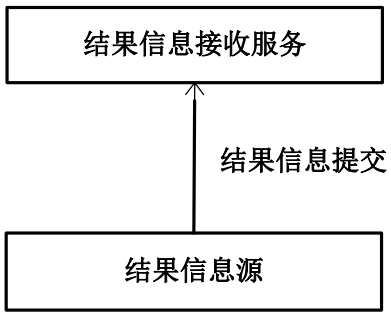

图48 结果信息接收服务角色交易图

结果信息接收活动主要有两类角色参与，结果信息接收服务和结果信息源。由结果信息源向结果信息接收服务提交结果信息。

7.2.5.1.2 角色的选择

表23　结果信息接收角色

角色	交易	选择
结果信息接收服务	结果信息提交	必须（R）
结果信息源	结果信息提交	必须（R）

7.2.5.1.3　交易流程

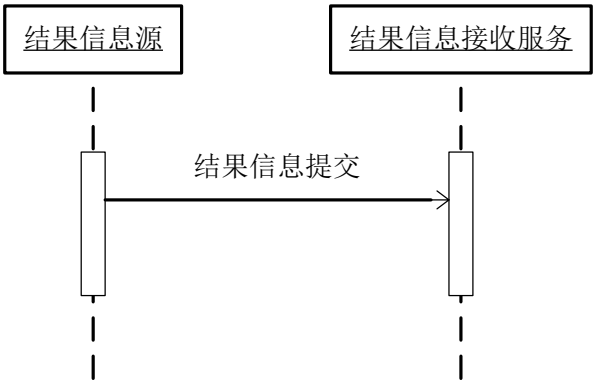

图49　结果信息接收服务时序图

- 结果信息源提交结果信息到结果信息接收服务；
- 结果信息接收服务校验数据并进行存储。

7.2.5.2　结果状态查询服务

7.2.5.2.1　角色和交易

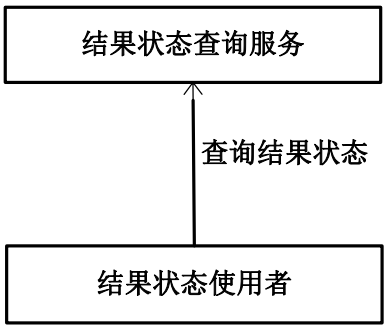

图50　结果状态查询服务角色交易图

7.2.5.2.2　角色的选择

表24　结果状态查询角色

角色	交易	选择

结果状态查询服务	查询结果状态信息	必须（R）
结果状态使用者	查询结果状态信息	必须（R）

7.2.5.2.3 交易流程

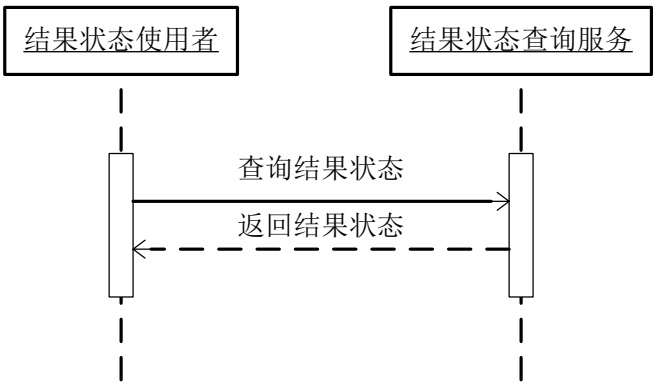

图51 结果状态查询服务时序图

- 结果状态使用者将查询结果状态信息请求提交到结果状态查询服务；
- 结果状态查询服务将查询结果返回给结果状态使用者。

7.2.5.3 结果信息查询

7.2.5.3.1 角色和交易

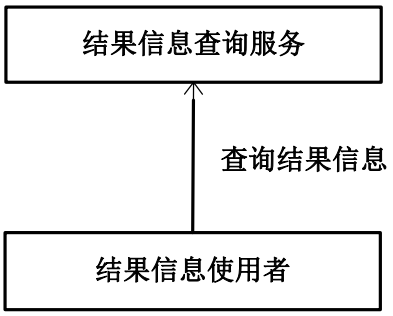

图52 结果信息查询服务角色交易图

7.2.5.3.2 角色的选择

角色	交易	选择
结果信息查询服务	查询结果信息	必须（R）

结果信息信息使用者	查询结果信息	必须（R）

7.2.5.3.3 交易流程

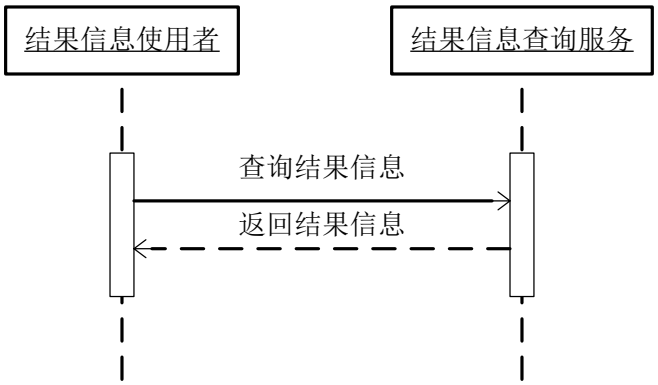

图53 结果信息查询服务交易时序图

- 结果信息使用者将查询结果信息请求提交到结果信息查询服务；
- 结果信息查询服务将查询结果返回给结果信息使用者。

7.2.5.4 结果信息发布服务

7.2.5.4.1 角色和交易

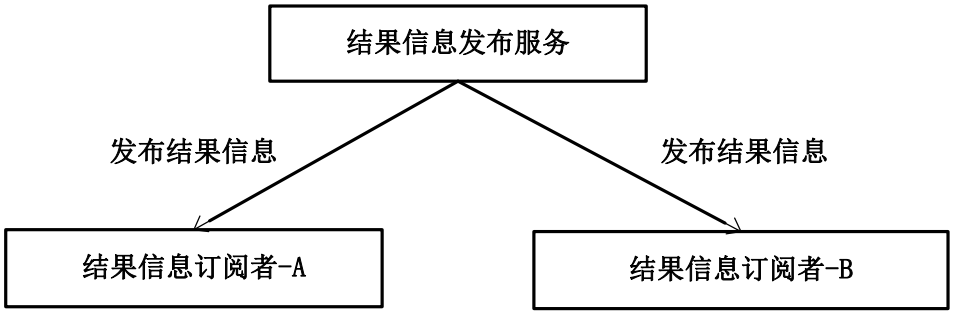

图54 结果信息发布服务角色交易图

7.2.5.4.2 角色的选择

表25 结果信息发布角色

角色	交易	选择
结果信息发布服务	结果信息发布	必须（R）
结果信息订阅者	结果信息发布	必须（R）

7.2.5.4.3 交易流程

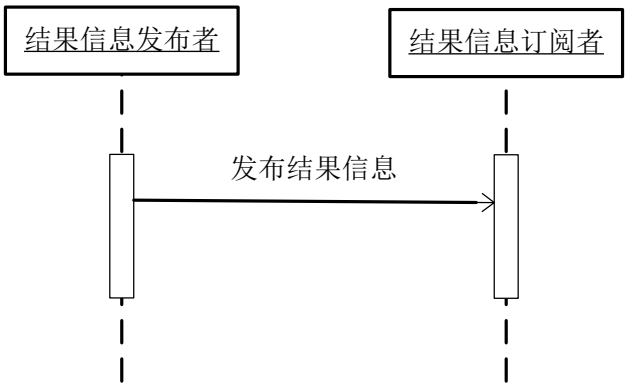

图55 结果信息发布服务时序图

- 结果信息发布者将结果信息发布给结果信息订阅者；
- 结果信息订阅者接收结果信息。

7.2.5.5 结果信息订阅服务

7.2.5.5.1 角色和交易

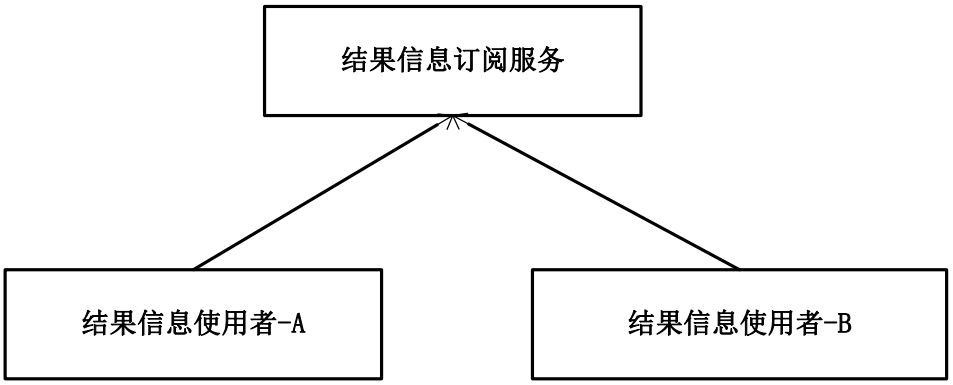

图56 结果信息订阅服务交易图

7.2.5.5.2 角色的选择

表26 结果信息订阅角色服务角色

角色	交易	选择
结果信息订阅服务	订阅结果信息	必须（R）
结果信息使用者	订阅结果信息	必须（R）

7.2.5.5.3　交易流程

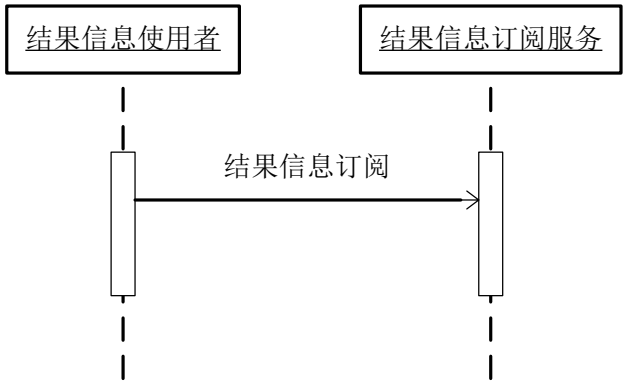

图57　结果信息订阅服务时序图

- 结果信息使用者订阅结果信息到结果信息订阅服务；
- 结果信息订阅服务校验数据并进行存储。

7.3　电子病历档案服务

7.3.1　电子病历文档索引服务

7.3.1.1　文档注册服务

7.3.1.1.1　角色和交易

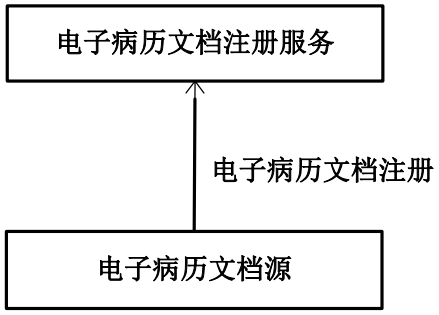

图58　电子病历文档注册服务服务角色交易图

电子病历文档注册活动主要有两类角色参与，电子病历文档注册服务和电子病历文档源。由电子病历文档源向电子病历文档注册服务注册电子病历文档。

7.3.1.1.2　角色的选择

表27　电子病历文档注册角色

角色	交易	选择
电子病历文档注册服务	电子病历文档注册	必须（R）
电子病历文档源	电子病历文档注册	必须（R）

7.3.1.1.3 交易流程

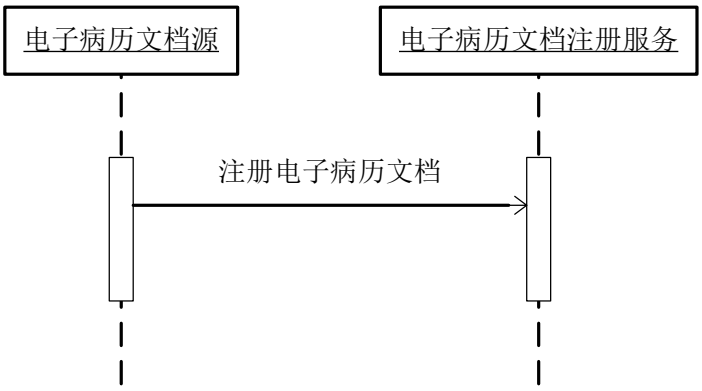

图59 文档注册服务时序图

- 电子病历文档源提交电子病历文档到电子病历文档注册服务；
- 电子病历文档注册服务校验数据并进行存储。

7.3.1.2 文档检索服务

7.3.1.2.1 角色和交易

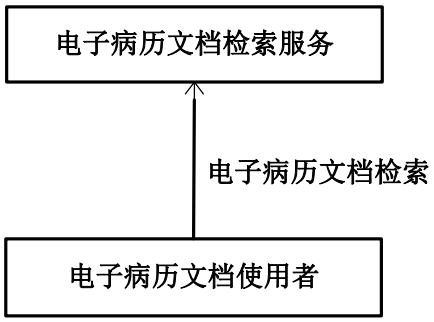

图60 电子病历文档检索服务服务角色交易图

电子病历文档检索活动主要有两类角色参与，电子病历文档检索服务和电子病历文使用者。由电子病历文档使用者向电子病历文档检索服务提交电子病历文档检索请求。

7.3.1.2.2 角色的选择

表28 电子病历文档检索角色

角色	交易	选择
电子病历文档检索服务	电子病历文档检索	必须（R）

电子病历文档使用者	电子病历文档检索	必须（R）

7.3.1.2.3 交易流程

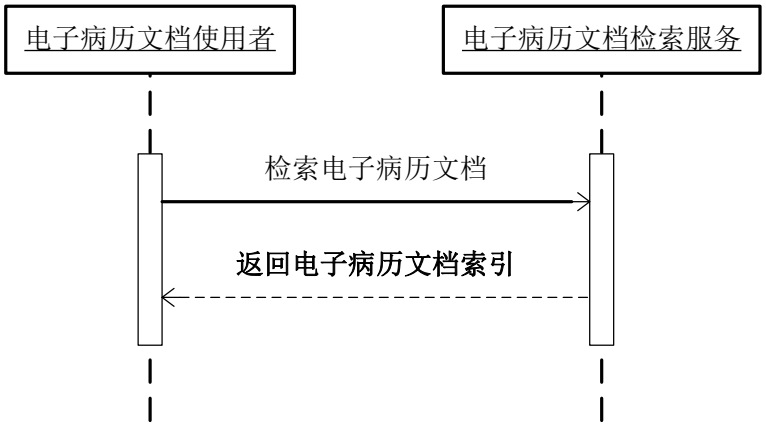

图61 电子病历文档检索服务时序图

- 电子病历文档使用者提交检索请求给电子病历文档检索服务；
- 电子病历文档检索服务将查询结果返回给电子病历文档使用者。

7.3.2 电子病历文档存储服务

7.3.2.1 电子病历文档接收服务

7.3.2.1.1 角色和交易

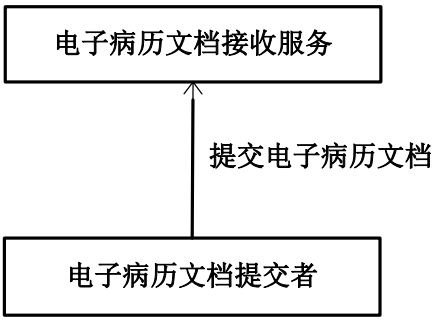

图62 电子病历文档接收服务角色交易图

电子病历文档接收活动主要有两类角色参与，电子病历文档接收服务和电子病历文档提交者。由电子病历文档提交者向电子病历文档接收服务提交电子病历文档。

7.3.2.1.2 角色的选择

表29 电子病历文档接收角色

角色	交易	选择
电子病历文档接收服务	提交电子病历文档	必须（R）
电子病历文档提交者	提交电子病历文档	必须（R）

7.3.2.1.3 交易流程

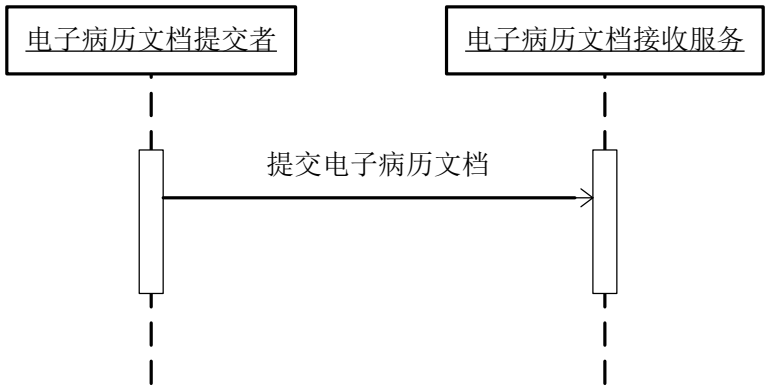

图63 电子病历文档接收服务时序图

- 电子病历文档提交者提交电子病历文档到电子病历文档接收服务；
- 电子病历文档接收服务校验数据并进行存储。

7.3.2.2 电子病历文档调阅服务

7.3.2.2.1 角色和交易

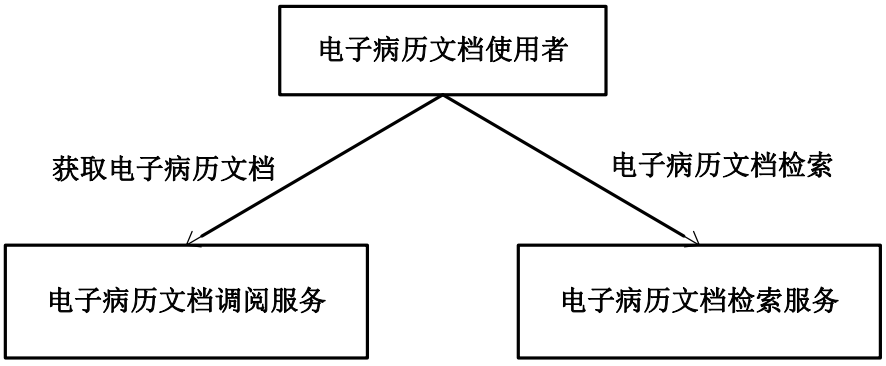

图64 电子病历文档调阅服务角色交易图

电子病历文档调阅活动主要有三类角色参与，电子病历文档检索服务、电子病历文档调阅服务和电子病历文档使用者。由电子病历文档使用者提交检索请求给电子病历文档检索服务，由电子病历文档检索服务返回文档索引，电子病历文档文档使用者通过电子病历文档调阅服务获取病历文档。

7.3.2.2.2 角色的选择

表30　电子病历文档调阅角色

角色	交易	选择
电子病历文档使用者	获取电子病历文档	必须（R）
电子病历文档检索服务	电子病历文档检索	必须（R）
电子病历文档调阅服务	提供电子病历文档	必须（R）

7.3.2.2.3　交易流程

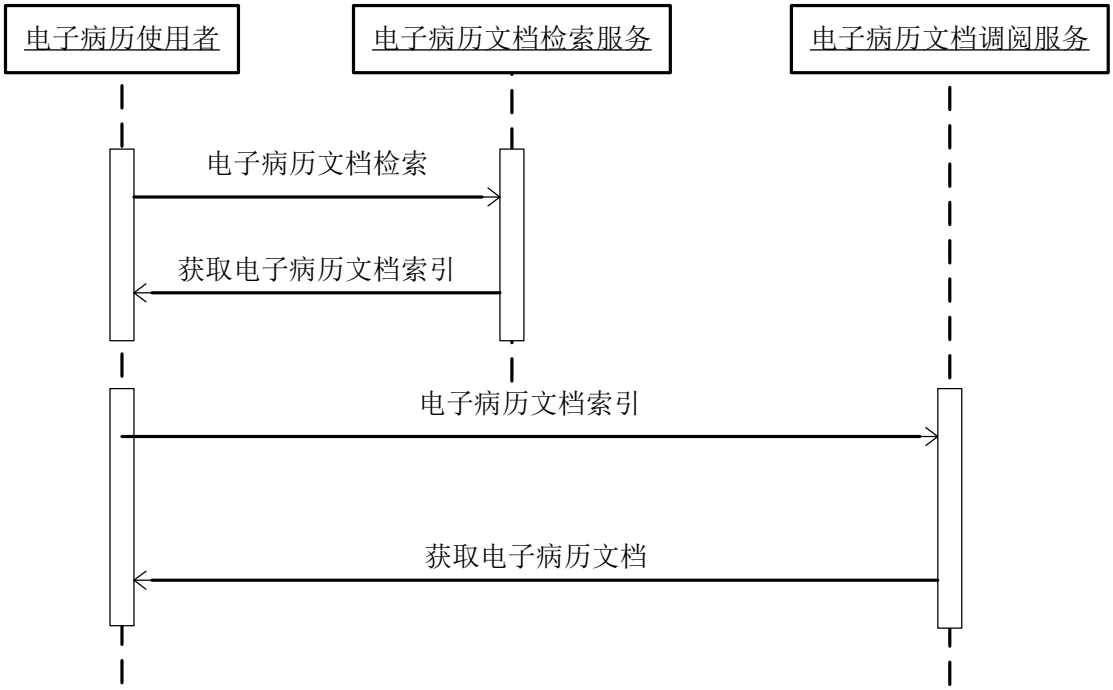

图65　电子病历文档调阅服务时序图

- 电子病历文档使用者提交检索请求给电子病历文档检索服务；
- 电子病历文档检索服务将查询结果返回给电子病历文档使用者；
- 电子病历使用者提交索引给电子病历文档调阅服务；
- 电子病历文档调阅服务将文档返回给电子病历文档使用者。

7.4　医院信息平台与区域卫生信息平台的交互服务

7.4.1　个人注册服务调用

7.4.1.1　个人身份注册服务

7.4.1.1.1　角色和交易

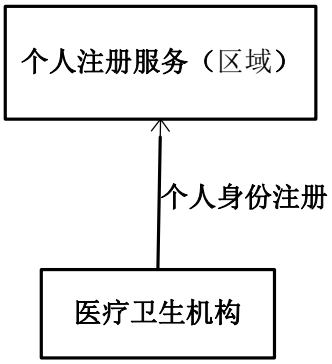

图66　注册服务调用角色交易图

7.4.1.1.2　角色的选择

表31　注册服务调用角色

角色	交易	选择
医疗卫生机构	个人身份信息新增	必须（R）
	个人身份信息修订	必须（R）
	个人身份信息合并	必须（R）
个人注册服务（区域）	个人身份信息新增反馈	必须（R）
	个人身份信息修订反馈	必须（R）
	个人身份信息合并反馈	必须（R）

7.4.1.1.3　交易流程

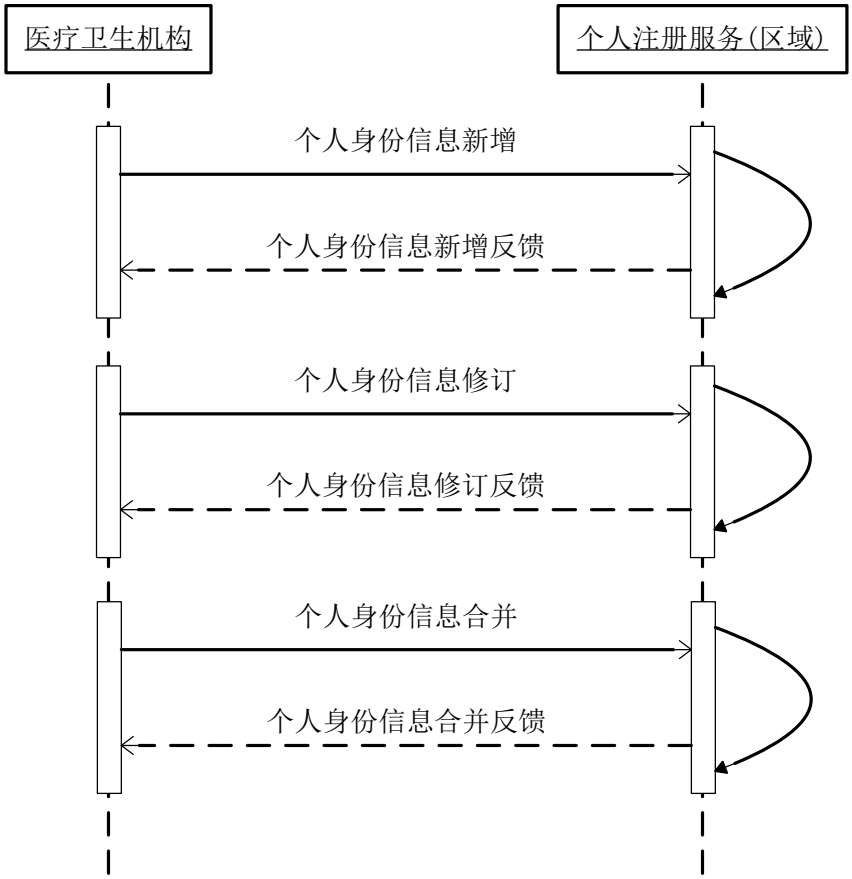

图67　个人注册服务调用时序图

- 医疗卫生机构向区域个人身份管理者提交个人身份信息新增、修订、合并操作要求；
- 区域个人身份管理者对个人身份源提交的个人信息建立交叉索引，并且返回操作结果。

7.4.1.2　个人 ID 查询服务

7.4.1.2.1　角色和交易

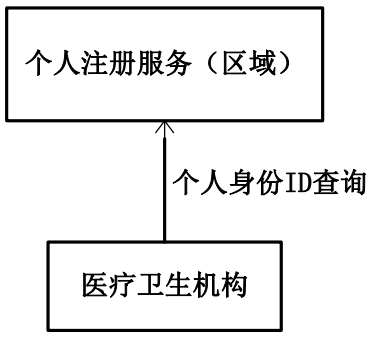

图68　个人 ID 查询服务调用角色交易图

7.4.1.2.2 角色的选择

表32 个人 ID 查询服务调用角色

角色	交易	选择
医疗卫生机构	个人 ID 查询	必须（R）
个人注册服务(区域)	个人 ID 查询反馈	必须（R）

7.4.1.2.3 交易流程

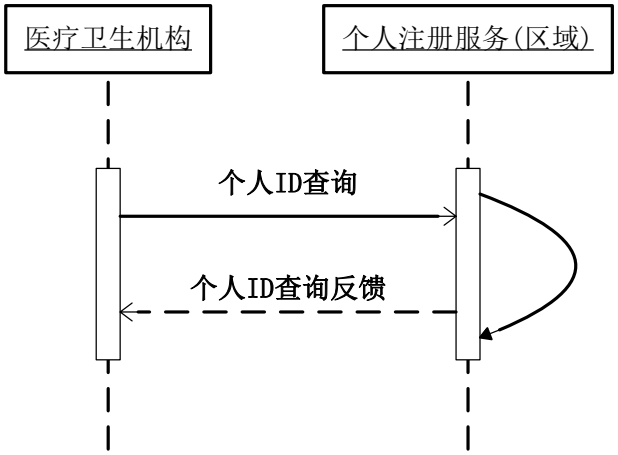

图69 个人 ID 查询服务调用时序图

- 医疗卫生机构向个人注册服务（区域）提交个人身份查询；
- 个人注册服务（区域）返回相关个人身份。

7.4.1.3 个人基本信息查询服务

7.4.1.3.1 角色和交易

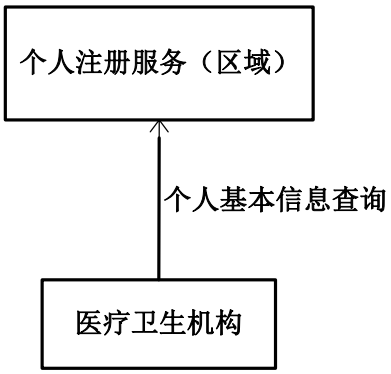

图70 个人基本信息查询服务调用角色交易图

7.4.1.3.2　角色的选择

表33　个人基本信息查询服务调用角色

角色	交易	选择
个人基本信息使用者	个人基本信息查询	必须（R）
个人注册服务(区域)	个人基本信息查询	必须（R）

7.4.1.3.3　交易流程

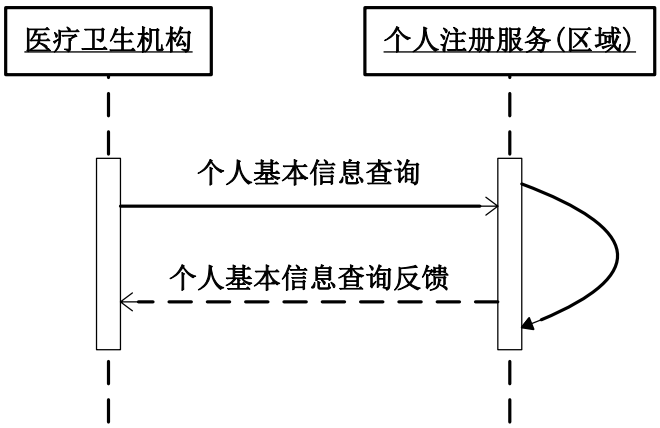

图71　个人基本信息查询服务调用时序图

- 医疗卫生机构向个人注册服务（区域）提交个人基本信息查询；
- 个人注册服务(区域)返回个人基本信息。

7.4.2　医疗卫生人员注册服务调用

7.4.2.1.1　角色和交易

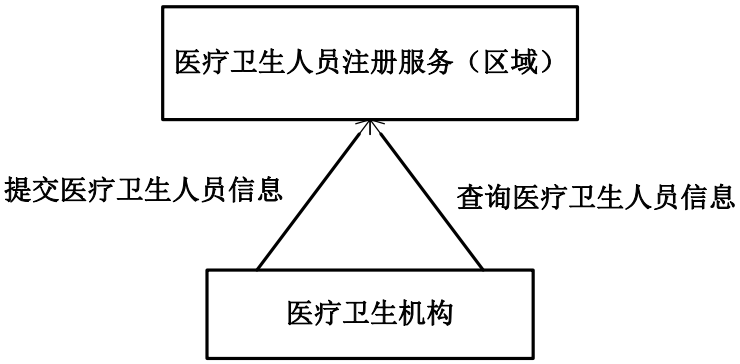

图72　医疗卫生人员注册服务调用角色交易图

7.4.2.1.2　角色的选择

表34　医疗卫生人员注册服务调用角色

角色	交易	可选性
医疗卫生机构	提交医疗卫生人员信息	必须(R)
	查询医疗卫生人员信息	
医疗卫生人员注册服务(区域)	提交医疗卫生人员信息	必须(R)
	查询医疗卫生人员信息	

7.4.2.1.3 交易流程

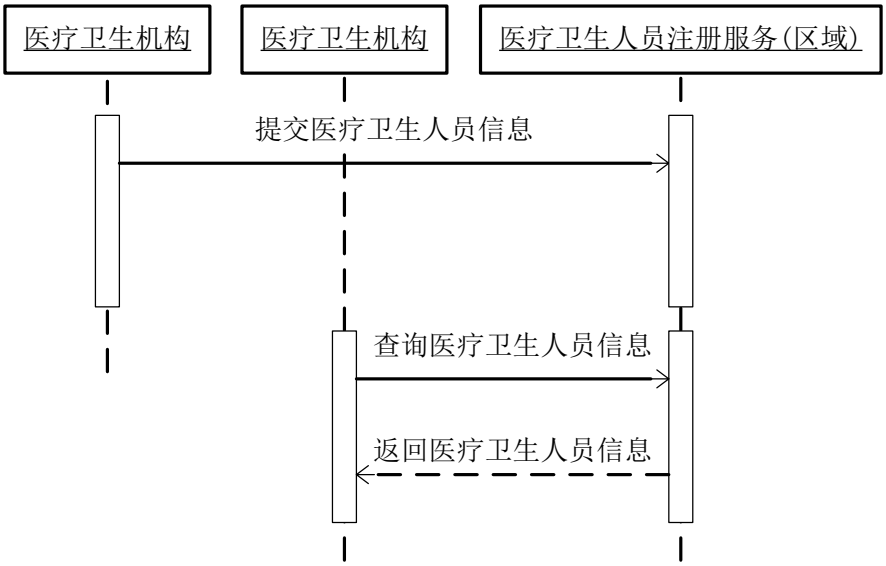

图73 医疗卫生机构注册服务调用时序图

- 机构向区域卫生信息平台中医疗卫生人员注册服务提交本机构的医疗卫生人员信息；
- 机构在某个跨机构的业务中，查询相关医疗卫生人员的信息。

7.4.3 医疗卫生机构注册服务调用

7.4.3.1.1 角色和交易

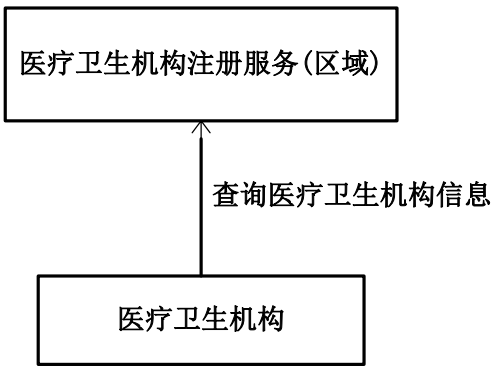

图74 医疗卫生机构注册服务调用角色交易图

7.4.3.1.2 角色的选择

表35 医疗卫生机构注册服务调用角色

角色	交易	可选性
医疗卫生机构	查询医疗卫生机构信息	必须(R)
医疗卫生机构注册服务(区域)	查询医疗卫生机构信息	必须(R)

7.4.3.1.3 交易流程

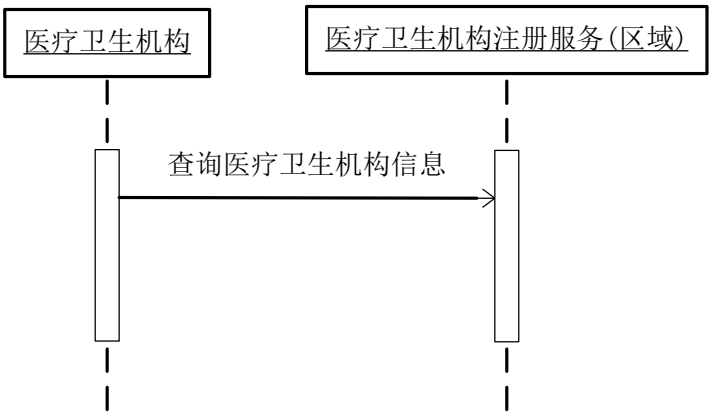

图75 医疗卫生机构注册服务调用时序图

- 机构在某个跨机构的业务中，查询相关医疗卫生机构的信息。

7.4.4 医疗卫生术语注册调用

7.4.4.1 注册、更新及版本管理

7.4.4.1.1 角色和交易

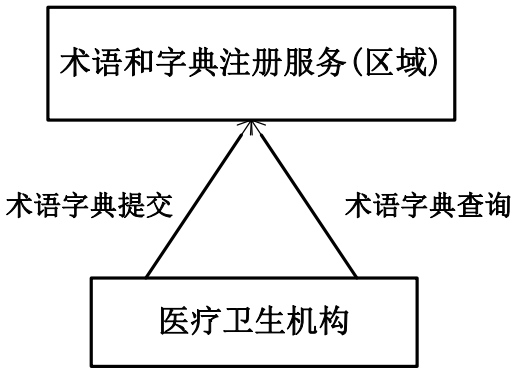

图76 医疗卫生术和语字典注册服务调用角色交易图

7.4.4.1.2 角色的选择

表36　医疗卫生术语和字典注册服务调用角色

角色	交易	选择
医疗卫生机构	术语字典提交	必须（R）
	术语字典查询	必须（R）
术语和字典注册服务(区域)	术语字典提交	必须（R）
	术语字典查询	必须（R）

7.4.4.1.3　交易流程

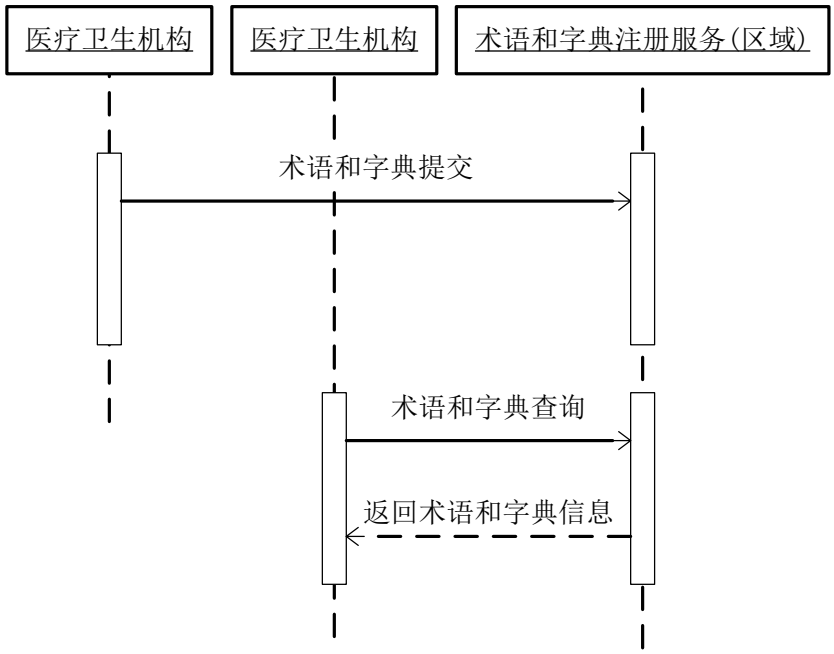

图77　医疗卫生术语和字典注册服务调用时序图

- 医疗卫生机构提交其原始术语和字典到术语字典注册服务（区域）；
- 术语和字典注册服务(区域)校验并进行相应的注册、更新、版本变更等行为。

7.4.4.2　术语和字典映射服务调用

7.4.4.2.1　角色和交易

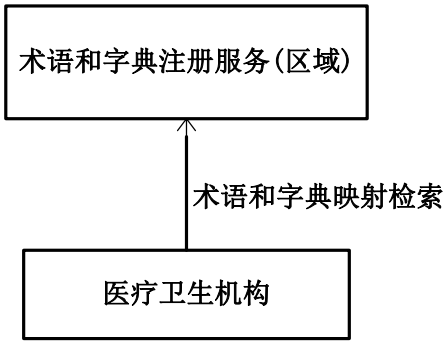

图78　术语和字典映射服务调用角色交易图

术语字典映射活动主要有两类角色参与，术语字典注册服务和医疗卫生机构（术语字典映射使用者）。由医疗卫生机构向术语字典注册服务（区域）提交术语和字典代码映射匹配检索请求，术语和字典注册服务（区域）返回相应的目标代码检索结果。

7.4.4.2.2　角色的选择

表37　术语和字典映射服务调用角色

角色	交易	选择
医疗卫生机构	术语和字典映射检索	必须（R）
术语和字典注册服务（区域）	术语和字典映射检索	必须（R）

7.4.4.2.3　交易流程

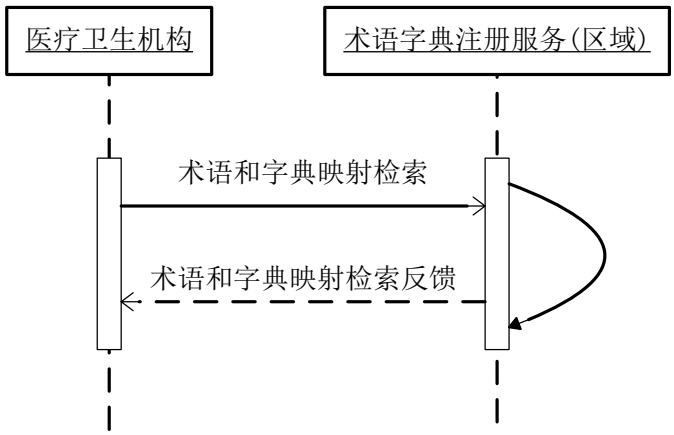

图79　术语和字典映射服务调用时序图

- 医疗卫生机构提交术语字典源代码检索请求；
- 术语和字典注册服务(区域)在术语字典库中检索目标代码，并将结果返回给医疗卫生机构。

7.4.5 健康档案调阅服务调用

7.4.5.1 调阅预判服务调用

7.4.5.1.1 角色和交易

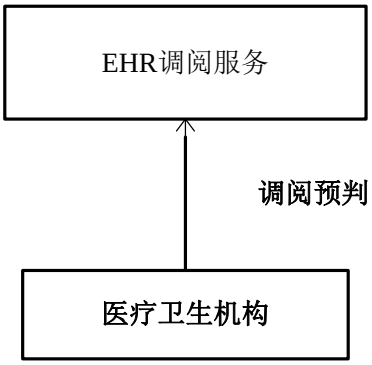

图80 调阅预判服务调用角色交易图

7.4.5.1.2 角色的选择

表38 调阅预判服务调用角色

角色	交易	选择
医疗卫生机构	调阅预判	必须（R）
EHR 调阅服务	调阅预判	必须（R）

7.4.5.1.3 交易流程

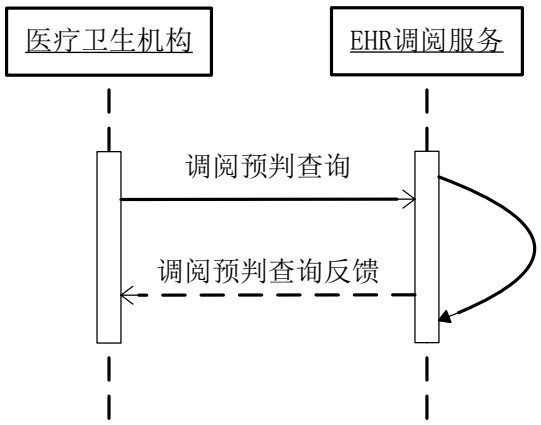

图81 调阅预判服务调用时序图

- 医疗卫生机构提交调用预判查询请求；
- EHR 调阅服务接收到请求后，判断是否存在居民的 EHR 数据，并把判断结果返回给医疗卫生机构。

7.4.5.2 调阅展示服务调用

7.4.5.2.1 角色和交易

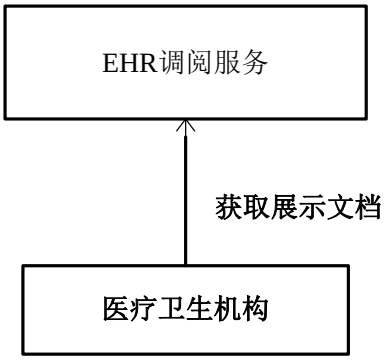

图82 调阅展示服务调用角色交易图

7.4.5.2.2 角色的选择

表39 调阅展示服务调阅服务角色

角色	交易	选择
医疗卫生机构	展示文档查询	必须（R）
EHR 调阅服务	获取展示文档	必须（R）

7.4.5.2.3 交易流程

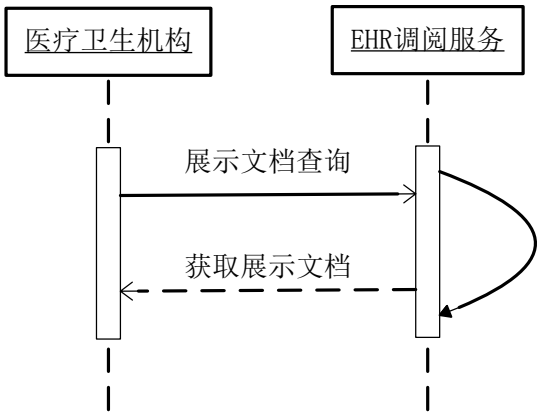

图83 调阅展示服务调用时序图

- 医疗卫生机构向 EHR 调阅服务提交展示文档请求；
- EHR 调阅服务将展示文档返回给医疗卫生机构。

7.4.5.3 调阅目录服务调用

7.4.5.3.1 角色和交易

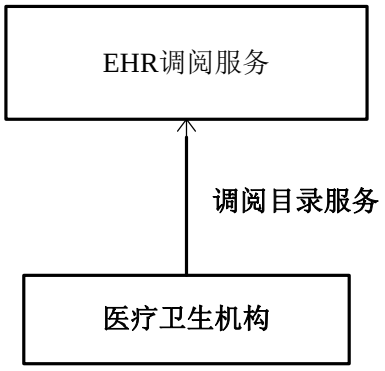

图84　调阅目录服务调用角色交易图

7.4.5.3.2　角色的选择

表40　调阅目录服务调用角色

角色	交易	选择
医疗卫生机构	调阅目录服务反馈	必须（R）
EHR 调阅服务	调阅目录服务	必须（R）

7.4.5.3.3　交易流程

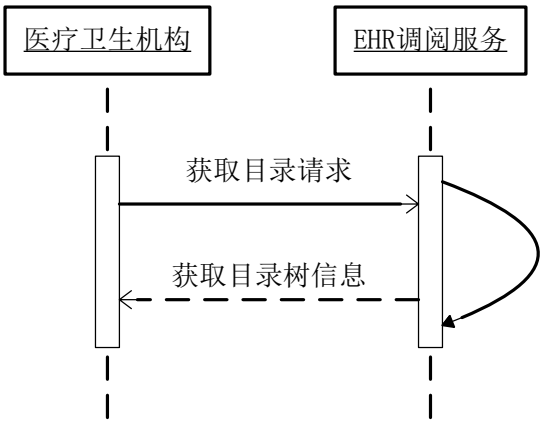

图85　调阅目录服务调用时序图

- 医疗卫生机构向 EHR 调阅服务提交获取文档目录请求；
- EHR 调阅服务将文档目录返回给医疗卫生机构。

7.4.5.4　摘要调阅服务调用

7.4.5.4.1　角色和交易

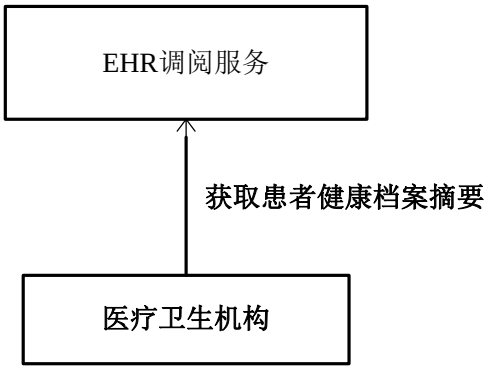

图86　调阅摘要信息服务调用角色交易图

7.4.5.4.2　角色的选择

表41　调阅摘要信息服务调用角色

角色	交易	选择
医疗卫生机构	反馈患者的健康档案摘要	必须（R）
EHR 调阅服务	获取患者健康档案摘要请求	必须（R）

7.4.5.4.3　交易流程

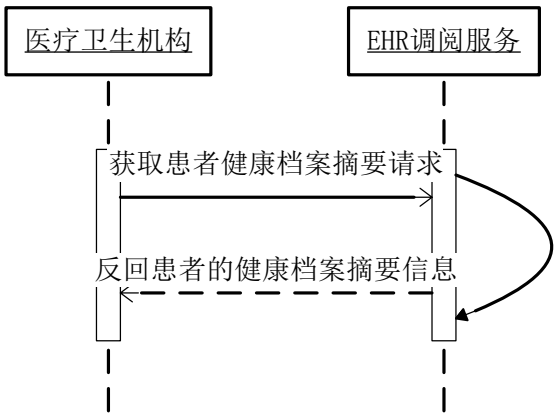

图87　调用摘要信息服务调用时序图

- 医疗卫生机构向 EHR 调阅服务提交获取患者居民健康档摘要请求；
- EHR 调阅服务将患者居民健康档摘要信息返回给医疗卫生机构。

7.4.6　病历文档上传服务调用

7.4.6.1.1　角色和交易

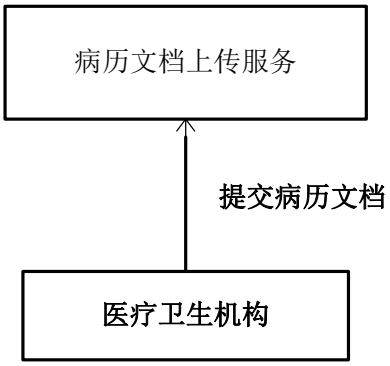

图88　病历文档上传服务调用角色交易图

7.4.6.1.2　角色的选择

表42　病历文档上传服务调用角色

角色	交易	选择
医疗卫生机构	提交病历文档	必须（R）
病历文档上传服务	提交病历文档	必须（R）

7.4.6.1.3　交易流程

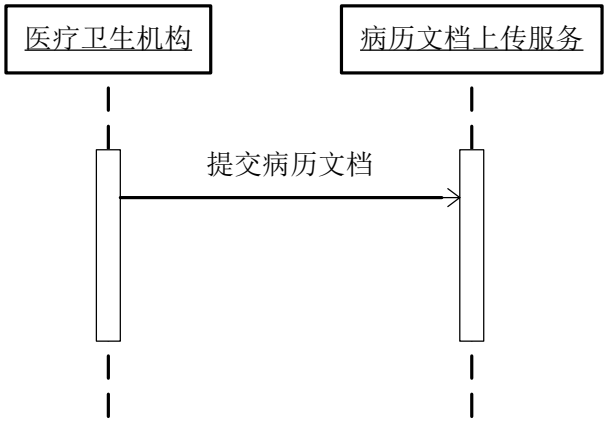

图89　病历文档上传服务调用时序图

- 医疗卫生机构向病历文档上传服务提交病历文档。

7.4.6.1.4　病历文档范围

参见WS XXX-2012 基于居民健康档案的区域卫生信息平台技术规范10.3.1。

7.4.7　病历数据查询服务调用

7.4.7.1.1　角色和交易

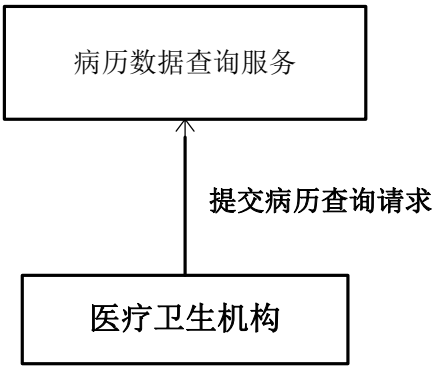

图90　病历数据查询服务调用角色交易图

7.4.7.1.2　角色的选择

表43　病历数据查询服务调用角色

角色	交易	选择
医疗卫生机构	提交病历数据查询请求	必须（R）
病历数据查询服务	提交病历数据查询请求	必须（R）

7.4.7.1.3　交易流程

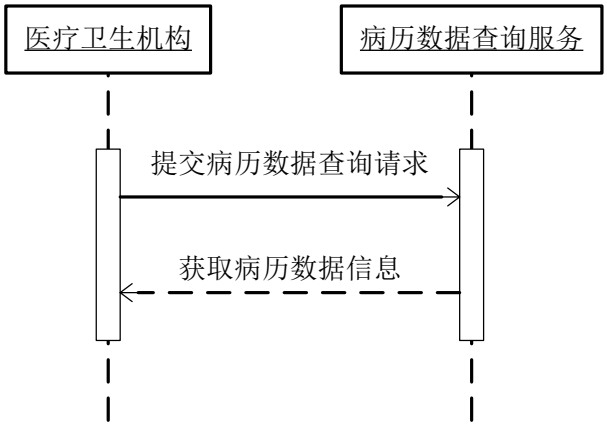

图91　病历数据查询服务调用时序图

- 医疗卫生机构向病历数据上传服务提交病历数据查询请求；
- 病历数据上传服务将病历数据信息返回给医疗卫生机构。

7.4.7.1.4　查询病历数据范围

参见WS XXX-2012 基于居民健康档案的区域卫生信息平台技术规范 10.3.1。

8　IT 基础设施规范

8.1 基本要求

用于搭建医院信息平台的IT基础设施（包括基础软件、数据库、服务器、存储、网络等），应满足一下基本技术要求：

a) 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；
b) 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；
c) 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；
d) 安全性要求:应遵循国内现有标准和规范要求，具体要求参照 9 安全规范。

8.2 基础软件

8.2.1 应用服务器

a) 系统基本要求
   1) 支持主流操作系统；
   2) 支持主流数据库系统；
   3) 支持主流服务器虚拟化软件系统；
   4) 支持主流消息中间件；
   5) 提供对应用开发的主流框架的支持；
   6) 支持 Web Service 最新标准和规范；
   7) 采用 J2EE 架构的应用服务器应通过 Java EE 5 兼容性认证，建议通过 Java EE 6 的兼容性认证；
   8) 兼容主流硬件服务器。
b) 可扩展性要求
   1) 具有良好的横向扩展能力，实现应用级负载均衡；
   2) 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。
c) 可用性要求
   1) 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；
   2) 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；
   3) 应实现 HTTP 会话级别的故障恢复；
   4) 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。

8.2.2 企业服务总线（ESB）

a) 系统基本要求
   1) 支持主流操作系统；
   2) 支持主流服务器虚拟化软件系统；
   3) 支持主流数据库系统；
   4) 支持 Web Service 最新标准和规范；
   5) 支持主流消息中间件；
   6) 提供对应用开发的主流框架的支持，提供主流编程语言的实现接口；
   7) 兼容主流硬件服务器。
b) 可扩展性要求
   1) 具有良好的横向扩展能力，实现负载均衡；

2） 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。

c） 可用性要求

1） 高稳定性，保证平台 7*24 小时的运行；

2） 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。

d） 功能要求

1） SOA 支持：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；

2） 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；

3） XML 支持：支持标准 XML 数据的格式转换，可以通过图形化映射组件、XSLT、客户化 Java 程序等多种方式实现转换功能；

4） 提供发布/订阅功能，支持队列和主题两种订阅模式；

5） 通讯协议支持：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。

8.3 数据库管理系统

用于搭建医院信息平台的数据库，应满足以下基本技术要求：

a） 系统基本要求

1） 支持主流操作系统；

2） 兼容主流硬件服务器，兼容主流存储架构；

3） 兼容主流的应用服务器架构；

4） 提供对应用开发的主流框架的支持，提供主流编程语言的实现接口。

b） 可扩展性要求

应具有横向可扩展性，支持多节点集群或者分布式部署，满足业务系统的处理能力需求。

c） 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
- 主备数据库或者数据库集群

d） 功能要求

1） 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；

2） 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；

3） 可选支持以压缩的形式存储数据；

4） 应支持 Unicode、GBK/GB2312 等多种字符集。

8.4 硬件服务器

8.4.1 基本要求

医院信息平台硬件服务器主要包括WEB服务器、应用服务器、数据库服务器等支撑医院信息平台的和各应用系统的运行所需的服务器。对于服务器支撑架构的技术要求主要包括：

a） 配置合理：服务器的资源配置（CPU、内存、硬盘、I/O 等）应该尽量与业务需求相匹配，实现资源的均衡使用；

b) 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；
c) 高可靠性要求：服务器各部件在提供足够性能的前提下，应具有良好的散热设计，良好的环境适应能力，并提供多种保护机制和冗余设计；
d) 管理自动化：服务器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、能耗、温度的监控，远程启动、访问和维护等。

8.4.2 系统要求

a) 支持主流操作系统；
b) 采用开放式架构和处理器；
c) 支持主流的内存型号,内存支持 ECC 纠错；
d) 支持普通硬盘或固态硬盘，并支持热插拔技术；
e) 支持磁盘阵列技术；
f) 支持多种主流存储架构，包括 FC SAN、IP SAN、NAS，可选支持 FCoE 技术；
g) 系统 I/O 插槽数量及集成网络端口数量可扩展；
h) 网络接口要求
- 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。

i) 供电：提供单电源/冗余电源可选。

8.4.3 可扩展性要求

服务器系统应满足可扩展性要求,建议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。

a) 横向扩展要求

服务器系统应具备组成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。应满足动态资源配置的要求。

b) 纵向扩展要求
- 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，可以通过内存扩展板进行扩展。
- 硬盘扩展能力：在一个机箱内支持多块硬盘槽位。支持 SATA/SAS/SSD 类型硬盘。
- 网卡扩展能力：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。

8.4.4 可靠性要求

对于医院内的一些重要业务系统，如：HIS、EMR、LIS等，采用数据库集群或者主备数据库模式部署，医院信息平台选择主机系统应具备多种高可用性保护措施，例如，内存ECC保护，硬盘RAID，冗余电源、可调频风扇等。具体包含：

a) 内存可靠性要求

主机系统应提供内存保护功能，为需要更高等级可用性的应用提供了增强的容错能力。用户将能够按照自己的意愿来选择系统内存保护级别：

1) 服务器内存提供 ECC 功能

2） 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

b） 硬盘可靠性要求

1） 应支持 RAID 技术，保证磁盘系统的高可靠性，提高持续工作而不发生故障的能力，包含但不限于：RAID0、1、0+1、5 等级别；

2） RAID 卡应支持缓存电池保护。

c） 整机可靠性要求

1） 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。用户可以按照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。

2） 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。

3） 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。

8.4.5 虚拟化技术支持

a） 虚拟化软件要求

1） 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。

2） 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。

3） 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。

4） 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，不同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。

5） 支持虚拟机的生命周期管理，包括虚拟机的创建、启动、暂停、恢复、重启、关闭等。

6） 支持虚拟机状态的监控，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。

7） 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。

8） 支持动态调度能力。当需要系统节能时，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。上述调度必须保证虚拟机内的服务不能停止。

9） 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。

10） 支持在主流分布式文件系统上创建虚拟机。

b） 主机对虚拟化支持要求

1） 主机能够支持主流的虚拟化软件；

2） 所有主机系统应支持同一个虚拟化引擎；

3） 处理器、I/O 和网络接口支持虚拟化硬件辅助功能。

8.4.6 服务器可管理性要求

服务器的管理体系应满足对医院信息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。

a） 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：

1） 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。

2） 配置管理

- 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。

3） 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）。

4） 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。

b） 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。

8.5 存储系统

8.5.1 基本要求

存储系统配置应结合医院内部和外部业务总体需求特点来考虑。存储系统应可以全方面满足医院信息平台建设需求。同时，存储系统在满足平台建设需求的前提下，尽量采用优化设计，应负责完成医院信息平台的业务连续性支持，并为医院快速发展和数据量高速膨胀打下一个良好的基础。

医院信息平台存储系统的基本技术要求包括：

a） 高可靠性：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。

b） 可扩展性： 根据医院未来业务的增长和变化，存储网络应可平滑扩充和升级，避免系统扩展时对存储网络架构的大幅度调整。

c） 灵活性和系统管理的简单性： 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。

d） 高性能：应保障网络存储设备的高吞吐能力，保证数据的高质量传输，保证在可预见的将来满足性能要求，避免网络瓶颈影响整体的系统应用。

e） 先进性和成熟性： 存储设备采用先进的技术和制造工艺，对于容量扩展支持、数据空间分配，抵御病毒攻击、高性能方面保持技术领先，网络结构和协议采用成熟的、普遍应用的并被证明是可靠的结构模型和技术。

f） 标准开放性： 支持国际上通用标准的网络存储协议、国际标准的应用的开放协议，保证与其它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。

g） 环保节能：应满足环保与节能的要求，噪声低、耗电低、无污染。

8.5.2 存储可靠性要求

存储系统需提供全年不断电无停止服务，确保高度的可靠性：全年不下电，不停机，不闪断。

a） 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；

b） 要求存储设备有 RAID 保护机制，在用户数据写单份的情况下，要求数据访问的可靠性达到 99.999%，即对单个存储节点要求；

c） 要求支持存储断电保护功能，并提供永久缓存数据保护；

d） 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；

e） 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；

f） 产品电位接地，防止触电事故；

g） 尺寸、规格、形状合理，以免倾斜倒伏，碰撞；
h） 产品材质耐温，散热；
i） 明确警示触电、有毒害、或其它危险发生的可能。

8.5.3 存储易管理性要求

a） 配有存储管理软件，能实现 FCSAN、IPSAN、NAS 一体化统一管理，提供全中文管理界面；
b） 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；
c） 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；
d） 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。

8.5.4 存储配置要求

8.5.4.1 中小型医院，存储配置要求

医院信息平台集中数据存储的基本要求，存储系统应能支持巨大的系统容量，可以集中存储不同平台的业务系统的数据。其中注册系统、索引系统、EMR交易缓存和EMR数据系统约为1到2TB/年，PACS等影像数据约为2到3TB/年。

存储配置要求：

a） 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；
- 冗余双控制器，提高存储安全性和存储系统与主机连接带宽；
- 可安装部署于多种操作系统并存的复杂网络环境中；
- 要求 FC\IP 主机连接，无缝接入用户现有应用环境；
- 全面支持 SAS、SATA 硬盘，实配容量≥5TB；最大扩展容量≥100TB，灵活配置满足不同层级数据存储需求；
- 高缓存，缓存≥4GB，最大缓存≥8GB；
- 集中部署，统一管理，降低整体拥有成本（TCO）。

b） 灾备系统要求
- 支持本地的连续数据保护功能，存储需要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；
- 支持数据本地卷复制、数据快照功能。

c) 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≥5TB，最多支持存储容量≥200TB
- 支持 LTO3\LTO4\LTO5 驱动器

8.5.4.2 大型医院，存储配置要求

医院信息平台集中数据存储的基本要求，存储系统应能支持巨大的系统容量，可以集中存储不同平台的业务系统的数据。其中注册系统、索引系统、EMR交易缓存和EMR数据系统约为3TB/年，PACS等影像数据约为5TB/年。

存储配置要求：

a) 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 IPSAN/FCSAN 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；
- 全面支持 SSD/FC/SAS/SATA 硬盘，支持 300/450/600GB 高转速 FC 磁盘；支持 300/450/600GB 高转速 SAS 磁盘，支持 500/1000/2000GB 高转速 SATAII 磁盘，支持 100GB SSD 硬盘，实配容量≥8TB；最大扩展容量≥200TB，灵活配置满足不同层级数据存储需求，
- 高缓存，缓存≥32GB，最大缓存≥64GB；
- 异构整合、集中部署，统一管理，降低整体拥有成本（TCO）。

b) 灾备系统要求
- 支持本地的连续数据保护功能，相对于传统的数据备份技术，存储需要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。

c) 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≥12TB，最多支持存储容量≥400TB
- 支持 LTO3\LTO4\LTO5 驱动器

8.6 网络与通信

8.6.1 医院信息网络设计基本要求

a) 可靠性要求：
- 网络系统需要支持 7×24 小时不间断运行
- 支持设备级的冗余备份
- 支持链路级的冗余备份

b) 安全性要求：
- 医院信息网络系统至少从逻辑上划为为内部网络和外部网络，内部网络和外部网络逻辑上需要进行隔离
- 内部网络主要承载医疗核心业务
- 外部网络主要提供行政办公服务、对外信息发布、医学资料查询服务

c) 灾备要求：
- 医院信息网络系统需要提供独立的灾备中心区
- 灾备中心区与数据中心区不能在同一物理位置

d) 模块化设计要求：

- 医院信息平台网络建设时应采用模块化、分区化、分层次设计

8.6.2 医院信息网络体系架构

8.6.2.1 网络分层要求

医院信息平台主要由两大部分组成，医院数据中心层和终端接入层。

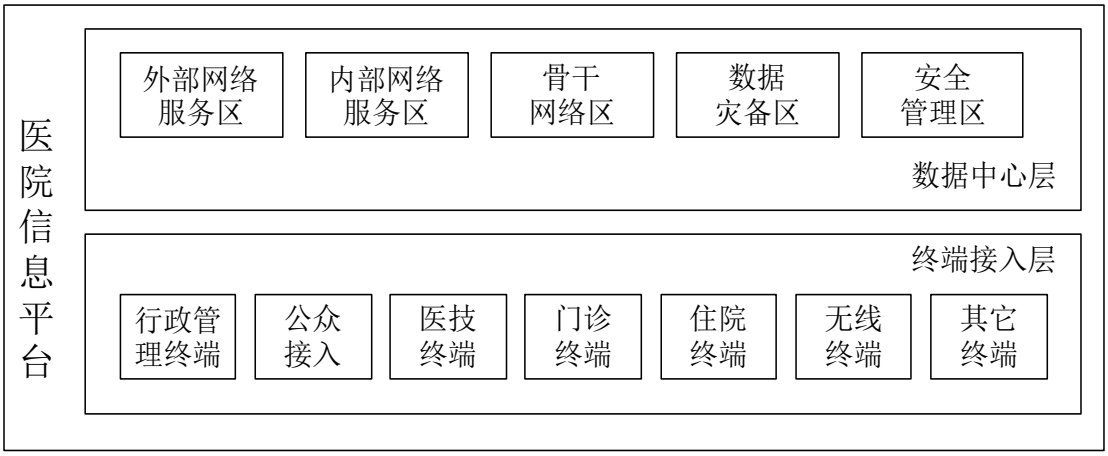

图92 网络架构分层模型

a) 终端接入层功能
- 负责将门诊、住院、医技、行政终端等接入网络
- 实现业务数据的提交
- 实现电子病历资源以及医疗信息的调用
- 并且为网上办公提供网络基础

b) 医院数据中心层
- 主要负责各业务系统的运行、管理
- EMR 信息的存储、调用
- 办公系统的业务支撑
- 医疗影像信息的存储
- 信息平台的外联

8.6.2.2 网络分区要求

a) 医院信息平台建议实际包含或功能上包含以下功能模块,可针对不同的区域运用不同的控制策略：

1) 内网中心服务器区
- 该区域是医院信息平台上内网业务系统相关设备的集中连接区域
- 该区域的服务器类型包括：应用服务器、数据库服务器、中间件服务器、数据存储设备等
- 该区域的业务系统类型包括：HIS 系统、LIS 系统，PACS 系统，EMR 系统等

2) 外网中心服务器区（DMZ 区）
- 该区域是一切外网业务系统相关设备的集中连接区域
- 该区域的服务器类型包括：应用服务器、数据库服务器、中间件服务器、数据存储设备等
- 该区域的业务系统类型包括：外网 OA 系统、外网 WEB 系统，MAIL 系统等

3) 数据灾备区

- 该区域是 HIS、电子病历、医学影像系统等数据中心子系统的灾备区域
- 业务系统与灾备区域数据要求能实时同步

4) 骨干网络区
- 该区域负责医院信息平台上数据中心区域内各服务器区之间的互联
- 该区域负责数据中心区与终端接入区之间的互联或汇聚互联
- 该区域实现局域网内数据的高速处理和转发

5) 医疗专网出口区
- 该区域主要功能为为医疗信息平台提供医疗专网的接入服务
- 医疗专网主要包括：医疗行业上级单位、疾控直报网络、公共卫生突发预警系统、公安局、区域医疗卫生信息平台等

6) 互联网出口区
- 该区域是为下载医学相关资料，获取互联网海量信息而提供的安全的 Internet 出口
- 该区域是医院的门户网站，是对公众社会提供服务的出口区域

7) 网络安全管理区
- 该区域是保障数据中心整体信息平台安全、稳定运行的安全管理运维系统的连接区域
- 该区域包括应用有：证书服务器、身份认证、漏洞扫描、入侵检测、网络管理等

8) 门诊终端接入区
- 该区域主要是将医院门诊部医疗相关的核心业务终端接入医院基础网络，提供门诊部医疗终端与数据中心之间的互联互通性
- 该区域主要包括门诊部门的医生工作站、护士工作站、计价终端系统等医疗相关终端系统接入

9) 住院终端接入区
- 该区域主要是将医院住院部医疗相关的核心业务终端接入医院基础网络，提供住院部医疗终端与数据中心之间的互联互通性
- 主要包括住院部门的医生工作站，护士工作站，住院部计价终端系统等医疗相关终端系统接入

10) 医技终端接入区
- 该区域主要是将医院医技终端接入医院基础网络，
- 该区域主要包括医学影像系统，医疗化验系统，医疗监护系统等

11) 无线终端接入区
- 该区域主要是将无线查房系统，医疗手持终端，无线监护系统等依赖无线网络的系统通过高速可靠的无线接入点，连入医院的基础网络

12) 行政终端接入区
- 该区域将医院的非医疗事务类行政终端接入网络的区域
- 该区域包含应用包括：协同办公、邮件、局域网即时通信

13) 其他终端接入区
- 该区域主要是将除上述终端以外的一些其他医生所用终端接入网络的区域

b) 网络分区互联要求
- 数据中心的各区域模块间通过独立的防火墙设备或者防火墙板卡进行安全隔离
- 医疗专网出口区需通过专线连接，应能够提供冗余的出口线路
- 内网中心服务器区和外网中心服务器区可通过二层隔离、三层隔离、安全域划分、MPLS VPN 等技术进行逻辑网络隔离

c) 无线终端接入区要求

- 需采用高速的无线网络连接，并且具备良好的技术后向兼容性 ；
- 需避免和医疗设备形成干扰；
- 需具有良好的信号覆盖性能 ；
- 需具有安全的无线网络接入 ；
- 需支持简单方便集中的管理方式 ；
- 需支持市电供电和 POE 供电两种模式。

8.6.2.3 网络架构设计要求

网络可靠性要求：

a) 设备级别可靠性要求
   - 网络设备需支持风扇冗余
   - 网络设备需支持电源冗余
   - 核心设备需提供关键部件的冗余备份，关键组件支持热插拔与热备份
   - 核心设备需支持引擎冗余，引擎自动切换
   - 核心设备需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
b) 网络级别可靠性要求
   - 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

8.6.3 网络管理要求

8.6.3.1 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，用户从可以从不同的角度浏览视图，实时了解和监控整个网络的运行情况。

拓扑管理需支持以下功能：

a) 拓扑图基础功能
   - 鸟瞰图：可方便定位拓扑窗口显示的区域
   - 全网网元统计：可统计全网网元类型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
b) 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
c) 支持拓扑自动发现：系统应提供拓扑自动发现，无需人工干预

8.6.3.2 性能管理

需要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

性能管理需支持以下几部分功能：

a) 监控实例管理
   - 用户可以按照预先设置的模板和定时策略对指定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
b) 监控模板管理

- 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。

c） 历史性能数据浏览：

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

8.6.3.3 安全管理

需要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。网管安全管理须支持以下几部分功能：

a） 登录和会话管理

b） 用户和用户组管理：

- 新建用户帐号和用户组管理
- 修改用户和用户组信息
- 删除用户帐号和用户组

c） 权限管理：

用户权限包括管理权限和操作权限

- 管理权限是指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；
- 操作权限是指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。

d） 安全策略管理：

- 设置密码策略用来设置用户密码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、超级用户密码长度最小值和密码长度最大值；
- 密码安全策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；
- 设置帐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。

e） 地址访问控制：

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

8.6.3.4 告警管理

告警管理需要对网络中的异常运行情况进行实时监视，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：

- 全网告警监视
- 告警统计
- 告警屏蔽和相关性分析
- 告警转储和确认

- 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别
- 告警抑制：某个告警为抑制状态后，后续不再上报该告警
- 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为网管本地时间
- 多种告警通知手段：支持电子邮件、短消息等告警远程通知

8.6.3.5 故障管理

a) 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
b) 故障采集应支持以下几种方式：
   - 支持直连方式采集：管理终端与待采集设备可通过网线或者串口线直接相连，通过 Telnet、SSH 或串口方式连接设备；
   - 支持自动代理方式采集：能够确定代理的设备类型时，选用自动代理；
   - 支持手工代理方式支持：不能确定代理的设备类型时，选用手工代理；
   - 支持“VPN 实例”方式支持：设备位于 VPN 私网中，选用 VPN 实例方式。

8.6.3.6 报表管理

网络管理系统需要能针对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。系统需产生以下基础类型报表：

a) 告警和日志类报表
   - 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
b) 资源类报表
   - 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

8.6.3.7 日志分析

系统需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。

日志分析需要支持的功能包括：

- 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，以便在解释库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，其他日志记录被隐藏
- 输入日志的解析：解析用户手工输入的日志，并且可以选择解释库，对解析后的日志进行解释

8.6.3.8 网络巡检

系统需依据网络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。

a) 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
   - 设备单板运行状况
   - 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

b) 巡检安排：
   - 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设备进行巡检和观察，监控设备和版本的运行情况，防止新问题出现。

8.7 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。从技术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/T 20988-2007 信息系统灾难恢复规范》的要求。

灾备建设的指标主要为RPO和RTO两种：

RPO：（Recovery Point Object）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系统当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。

医院信息系统包含HIS、LIS、RIS、电子病历、PACS等临床信息系统，各系统的正常运行与医院的经营息息相关，而且产生海量的不容丢失的数据。为保证医院信息系统正常、安全运转，在硬件基础设施中，必须配置备份或容灾系统。

表44　医院灾备系统 RTO/RPO 等级要求

			医院规模		
灾难恢复等级	恢复时间（RTO）	可接受的数据丢失（RPO）	小型医院	中型医院	大中型医院
AAA	0.5 小时或更少	最大 0.5 小时			电子病历、ODS、数据仓库
AA	0.5-2 小时	2 小时		电子病历，ODS	
A	2-4 小时	4 小时	电子病历、ODS	数据仓库	
B	4-72 小时	24 小时	数据仓库		

- 小型医院，HIS、电子病历、ODS 等系统的灾备建设要求是：RTO≤4 小时，RPO≤4 小时；LIS、RIS、PACS 等系统的在被建设目标是：RTO≤72 小时，RPO≤24 小时。
- 中型医院，HIS、电子病历、ODS 等系统的灾备建设要求是：RTO≤2 小时，RPO≤2 小时；数据仓库、LIS、RIS、PACS 等系统的在被建设目标是：RTO ≤4 小时，RPO≤4 小时。
- 大型医院，HIS、电子病历、ODS 等系统的灾备建设要求是：RTO≤0.5 小时，RPO≤0.5 小时；数据仓库、LIS、RIS、PACS 等系统的在被建设目标是：RTO ≤2 小时，RPO≤2 小时。

8.8　机房环境

应遵循国内标准和规范，并参考国际上现有的标准和规范。

9　安全规范

9.1　安全设计原则

a)　规范性原则

安全设计应遵循已颁布的相关国家标准。

b)　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。

c)　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。

d)　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，安全子系统可以不作修改或少量修改就能在新环境下运行。

e)　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。

f） 系统性原则

应综合考虑安全子系统的整体性、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。

g） 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。

9.2 总体框架

a） 医院信息平台安全体系从安全技术、安全管理为要素进行框架设计；
b） 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；
c） 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。

9.3 技术要求

9.3.1 物理安全

物理安全主要是指医院信息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。

a） 物理位置的选择
- 应满足 GB/T 22239-2008 中 7.1.1.1 的要求

b） 物理访问控制
- 应满足 GB/T 22239-2008 中 7.1.1.2 的要求

c） 防盗窃和防破坏
- 应满足 GB/T 22239-2008 中 7.1.1.3 的要求

d） 防雷击
- 应满足 GB/T 22239-2008 中 7.1.1.4 的要求

e） 防火
- 应满足 GB/T 22239-2008 中 7.1.1.5 的要求

f） 防水和防潮
- 应满足 GB/T 22239-2008 中 7.1.1.6 的要求

g） 防静电
- 应满足 GB/T 22239-2008 中 7.1.1.7 的要求

h） 温湿度控制
- 应满足 GB/T 22239-2008 中 7.1.1.8 的要求

i） 电力供应
- 应满足 GB/T 22239-2008 中 7.1.1.9 的要求

j） 电磁防护
- 应满足 GB/T 22239-2008 中 7.1.1.10 的要求

9.3.2 网络安全

9.3.2.1 基础网络安全

a） 结构安全

- 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本规范 8.5 要求。

b) 网络设备防护

- 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。

9.3.2.2 安全区域边界安全

a) 在医院信息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 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，并且可以对审 计事件提供的告警；
- 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、SMTP、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。

b) 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。

c) 应在在平台和外部网络边界处对恶意代码进行检测和清除：

- 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部署恶意代码检测系统。

9.3.2.3 安全审计

a) 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。

9.3.3 服务端系统安全

9.3.3.1 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查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：

a) 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
   - 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，口令设置必须具备一定的复杂度，不合格的口令被拒绝；口令必须具备采用 3 种以上字符、长度不少于 8 位，并设置定期更换要求；
b) 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；
c) 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；
d) 当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听；
e) 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：
   - 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。

9.3.3.2 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：

a) 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；
b) 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；
c) 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；
d) 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；
e) 应对重要信息资源设置敏感标记；
f) 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；
g) 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；

h) 应能够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。

9.3.3.3 安全审计

在管理区域部署审计系统，对医院信息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：

a) 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；
b) 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。
c) 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；
d) 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
e) 应能够根据记录数据进行分析，并生成审计报表；
f) 应保护审计进程，避免受到未预期的中断。

9.3.3.4 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：

a) 远程控制与管理
b) 保持操作系统补丁及时得到更新
c) 全网查杀毒
d) 防毒策略的定制与分发实时监控
e) 客户端防毒状况
f) 病毒与事件报警
g) 病毒日志查询与统计
h) 集中式授权管理
i) 全面监控邮件客户端

9.3.3.5 剩余信息保护

a) 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除，无论这些信息是存放在硬盘上还是在内存中；
b) 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。

9.3.3.6 入侵防范

a) 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；
b) 应能够检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；
c) 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。

9.3.4 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/硬件需具备以下功能：

a) 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
b) 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；
c) 应对系统中的重要终端进行审计，审计粒度为用户级；
d) 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它与审计相关的信息；
e) 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；
f) 应保护审计进程，避免受到未预期的中断；
g) 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；
h) 应定期对审计记录进行分析，以便及时发现异常行为；
i) 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；
j) 宜支持多操作系统，分离不同类型的应用场景；
k) 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。

9.3.5 应用安全

9.3.5.1 用户管理和权限控制

a) 应确保访问医院信息平台的所有实体（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：
   - 对医院信息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）；
   - 确保每个用户必须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，则系统也必须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必须是不可伪造；
   - 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）。
b) 应根据用户对医院信息平台系统的使用性质的不同进行用户分类管理：
   - 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。
c) 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：
   - 应支持基于“用户－角色/用户组－应用资源”的授权模型，制定授权策略；
   - 确保每个授权用户必须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、修改电子病历访问规则，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），满足电子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；
- 必须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。

9.3.5.2 信息安全

9.3.5.2.1 身份认证

a) 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：
   - 基于 PKI 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 USB Key 并进行 PIN 口令保护、私钥和 PIN 码应在 USB Key 内生成；
   - 用户名/口令认证方式：口令设置必须具备一定的复杂度、口令设置定期更换要求、口令字符输入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。
b) 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：
   - 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，必须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；
   - 必须对身份鉴别失败事件进行审计跟踪。
c) 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。
d) 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。

9.3.5.2.2 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：

- 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；
- 应能够对单个帐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。

9.3.5.2.3 关键业务抗抵赖

a) 系统执行关键业务操作时，对参与者/操作者发生动作时（如：初始录入、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,实现对对关键信息或操作的数字签名以及可视化展现。
b) 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
   - 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。
c) 应支持对数字签名信息加盖时间戳,时间戳必须由国家法定时间源来负责保障时间的授时和守时监测。

9.3.5.2.4 数据完整性保护

a) 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
b) 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
c) 应保障交换数据的真实性及不可抵赖性：
   - 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
d) 应确保电子病历中的每个条目必须是编写者签署，不应出现由其他人签署：
   - 宜采用数字签名/验签技术实现
e) 应提供电子病历的编写者进行电子病历的验证功能：
   - 宜采用数字签名/验签技术实现；
   - 应标明电子病历是否被验证；
   - 验证过程记录的文件要有保留。

9.3.5.3 隐私保护

a) 应提供数据保密等级服务：对电子病历设置保密等级的功能,对操作人员的权限实行分级管理，用户根据权限访问相应保密等级的电子病历资料。授权用户访问电子病历时，自动隐藏保密等级高于用户权限的电子病历资料；
b) 应提供数据访问警示服务：当医务人员因工作需要查看非直接相关患者的电子病历资料时，警示使用者要依照规定使用患者电子病历资料；
c) 应支持对电子病历数据的创建、修改、删除等任何操作都将自动生成、保存审计日志；
d) 应支持对关键个人病历信息（字段级、记录级、文件级）进行加密存储保护；
e) 应提供患者匿名化处理服务：提供对电子病历进行患者匿名化处理的功能，以便在必要情况下保护患者健康情况等隐私；

f) 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， 并将这些需求应用到医院信息平台环境中。在提供访问或传输患者电子病历等医疗数据之前，该服务应用于电子病历以确定患者或个人的许可指令是否允许或限制这些医疗数据的公开。

9.3.5.4 审计追踪

a) 应支持基本的行为审计记录功能：
   - 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。
b) 应支持对安全信息的统计分析：
   - 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。
c) 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。

9.3.5.5 剩余信息保护

a) 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；
b) 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。

9.3.5.6 软件容错

a) 应提供数据有效性检验功能，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；
b) 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。

9.3.6 数据安全及备份恢复

a) 应能检测到系统管理数据、身份鉴别信息、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
   - 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。
b) 应对身份鉴别信息、电子病历等重要业务数据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。

c） 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：

- 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进行应用数据备份，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；
- 故障恢复前应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。

9.4 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。

a） 安全管理制度
- 应满足 GB/T 22239-2008 中 7.2.1 的要求

b） 安全管理机构
- 应满足 GB/T 22239-2008 中 7.2.2 的要求

c） 人员安全管理
- 应满足 GB/T 22239-2008 中 7.2.3 的要求

d） 系统建设管理
- 应满足 GB/T 22239-2008 中 7.2.4 的要求

e） 系统运维管理
- 应满足 GB/T 22239-2008 中 7.2.5 的要求

10 性能要求

10.1 最小接入系统数

接入系统指接入医院信息平台的独立应用系统，如PACS、LIS等。

a） 对二级医院医院信息平台，允许最小接入系统数大于等于 3 个。

b） 对三级医院医院信息平台，允许最小接入系统数大于等于 6 个。

10.2 最小并发用户数

a） 对二级医院基于医院信息平台的应用系统，总的允许最小并发用户数大于 200。

b） 对三级医院基于医院信息平台的应用系统，总的允许最小并发用户数大于 600。

10.3 基础服务平均响应时间

a） 个人注册服务调用，单个患者注册平均响应时间小于 1 秒。

b） 个人基本信息查询，总记录 50 万以上，按患者唯一标识查询单个患者查询平均响应时间小于 2 秒；总记录 100 万以上，按患者唯一标识查询单个患者查询平均响应时间小于 3 秒。

c) 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，返回记录数小于 10 条时，平均响应时间小于 10 秒；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 15 秒。

10.4 电子病历整合服务平均响应时间

a) 就诊信息查询，总记录 50 万以上，按患者唯一标识查询,单个患者查询平均响应时间小于 2 秒；总记录 100 万以上，按患者唯一标识查询，单个患者查询平均响应时间小于 3 秒。
b) 就诊信息接收，单次患者就诊信息保存平均响应时间小于 1 秒。
c) 医嘱信息查询，总记录 500 万以上，按患者就诊号（一次就诊标识号）查询，返回记录数小于 10 条时，平均响应时间小于 3 秒；总记录 1000 万以上，返回记录数小于 10 条时，平均响应时间小于 4 秒。
d) 医嘱信息接收，每次提交小于 10 条时，平均响应时间小于 3 秒。
e) 申请单查询服务，按一个申请单标识号查询，平均响应时间小于 2 秒。
f) 申请单接收服务，平均响应时间小于 2 秒。
g) 预约查询服务，按一个预约标识号查询，平均响应时间小于 2 秒。
h) 预约接收服务，平均响应时间小于 1 秒。
i) 结果查询服务，按一个结果标识号查询，平均响应时间小于 2 秒。
j) 结果接收服务，平均响应时间小于 2 秒。

10.5 电子病历档案服务平均响应时间

a) 电子病历文档存储服务，提交单个模板电子病历文档实例时，平均响应时间小于 1 秒。
b) 电子病历文档索引查询，按患者唯一标识查询,返回患者电子病历文档目录树时，平均响应时间小于 2 秒。
c) 电子病历文档查询，按电子病历文档标识查询，平均响应时间小于 2 秒。

10.6 网络性能要求

a) 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。

b) 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
- 支持多种负载均衡算法、提供完全的第 4～7 层服务器负载均衡功能
- 支持 AH 和 ESP 两种 IPSec VPN 模式

c) 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和网络处理器热补丁

d) 入侵检测性能要求

- 处理能力 ≥ 200M
- 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
- 支持解析 SSL 加密通讯，可分析基于 SSL 加密的各种协议，包括 SMTP-over-SSL、POP3-over-SSL、TELNET-over-SSL、FTP-over-SSL、HTTPS 等
- 支持会话回放，可对 HTTP、TELET、FTP、SMTP、POP3 等会话进行实施监控并可以回放会话行为