ICS 11.020
C 07

WS

中 华 人 民 共 和 国 卫 生 行 业 标 准

WS/T XXXXX—2015

省级人口健康综合管理信息平台技术规范

Technical specification for Regional Health Information Platform based on EHR

（征求意见稿）

2015－XX－XX 发布　　2015－XX－XX 实施

国家卫生和计划生育委员会　　发 布

目　　次

前　言

本标准的附录A，附录B是资料性附录。
本标准由国家卫生计生委统计信息中心提出并归口
本标准的主要起草单位：
本标准的主要起草人：

引　言

本规范用于指导、规范和约束“省级人口健康综合管理平台”项目建设的具体功能和技术实现方式。并作为《省级人口健康综合管理平台功能测评方案》的重要依据。省级人口健康综合管理平台基础服务的技术实现的标准化文档，对省级人口健康综合管理平台建设开展测试、验收和评价工作提供指导。

本规范的主要对象是卫生局的区域卫生信息项目相关负责人，区域卫生信息服务提供商，卫生信息化专家，卫生信息化研究人员。

本规范的第4、5章，描述省级人口健康综合管理平台的整体架构。第6章，描述省级人口健康综合管理平台的基础功能和交易规范。第7章，描述省级人口健康综合管理平台的数据采集规范。第8章，描述省级人口健康综合管理平台的IT基础设施规范。第9章，描述省级人口健康综合管理平台的安全规范。第10章，描述省级人口健康综合管理平台的机构接入规范。第11章，描述省级人口健康综合管理平台基础服务的性能要求。

本规范描述了的省级人口健康综合管理平台基础服务的技术实现，由于受时间和技术的限制，以及技术的发展和卫生业务的拓展，省级人口健康综合管理平台的实现技术根据实践不断完善。我们将保持对于卫生信息化发展的关注，持续对于本规范的版本更新，确保省级人口健康综合管理平台的先进性。

基于居民健康档案的省级人口健康综合管理平台技术规范

1 范围

本规范是在WS/T 448-2014 基于健康档案的区域卫生信息平台技术规范的基础上以适应省级人口健康综合管理的需求为导向，进一步约束在省级人口健康综合管理平台项目的技术实现。是下一步编写《省级人口健康综合管理平台功能测评方案》的重要基础。

本规范进一步提出了基于居民健康档案的省级人口健康综合管理平台的技术架构，明确了省级人口健康综合管理平台注册服务、健康档案整合服务、健康档案存储服务、健康档案管理服务、健康档案调阅服务、健康档案协同服务、省级人口健康综合管理平台信息安全与隐私保护等关键技术实现，定义了功能规范、数据采集规范、交易流程规范、IT基础设施规范和安全规范，对省级人口健康综合管理平台IT基础设施建设提出机构接入要求和性能要求等，保证省级人口健康综合管理平台的服务提供。

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/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

HJ 2507-2011 环境标志产品技术要求 网络服务器

WS 363（所有部分） 卫生信息数据元目录

WS 364（所有部分） 卫生信息数据元值域代码

WS 365 城乡居民健康档案基本数据集

WS/T 447-2013 基于电子病历的医院信息平台技术规范

WS/T 448-2014 基于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）

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

基于居民健康档案的区域卫生信息平台 regional health information platform based on EHR

区域卫生信息平台 regional health information platform

连接区域内的医疗卫生机构基本业务信息系统的数据交换和共享平台，不同系统间进行信息整合的基础和载体。在本规范中特指地市级或区县级区域卫生信息平台。

3.1.2

省级人口健康综合管理平台 provincial population health management platform

在省一级搭建的基于区域卫生信息平台的综合管理平台。

3.1.3

信息资源中心 information resource center

省级人口健康综合管理平台信息资源中心

汇聚省内医疗卫生机构产生的以全员人口、健康档案、电子病历为核心的业务、管理、服务等信息资源，供省级人口健康综合管理平台及区域内医疗卫生机构使用。

3.1.4

居民resident

个人person

患者 patient

本规范中患者、居民和个人具有相同的意义，指通过医疗卫生服务体系获取和接受服务的个体。

3.1.5

交易

信息系统之间交互的一次过程。

3.1.6

角色actor

信息系统在一次交易过程中所承担的角色。

3.1.7

电子健康档案 electronic health record

健康档案 electronic health record

电子健康记录 electronic health record

电子化的健康档案，是关于医疗保健对象健康状况的信息资源库，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，各级授权用户均可访问。

3.1.8

信息安全 information security

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。

3.1.9

服务点系统 point of service system

接入省级人口健康综合管理平台的应用软件系统。主要包括医院信息系统、基层医疗卫生信息系统和公共卫生信息系统等。

3.1.10

基层医疗卫生机构 point of primary health service

社区卫生服务中心和站点、乡镇卫生院和村卫生室。

3.1.11

交易 transaction

角色之间某个特定服务的调用或反馈。

3.1.12

简单统计报表查询 simple statistics report query

仅在一张数据表中，利用主键或索引进行count或sum查询，不涉及表与表之间的关联。

3.1.13

单项统计 single item statistic

对于任何一个单一指标的统计计算。

3.1.14

复合汇总统计composite summary statistic

对多个上述“单项统计”指标结果的汇总。

3.1.15

复杂统计报表 complex statistics report

仅在多张数据表中，进行计数、加和等查询。可能涉及多表之间的相互关联。

3.2 缩略语

下列术语和定义适用于本文件。

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

BRE：Business Rules Engine，业务规则引擎

CDA：Clinical document Architecture，临床文档架构

CEP: complex event processing，复合事件处理

CIFS：Common Internet File System,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的一种协议

CIS：Clinical Information System，临床信息系统

CLI：command-line interface，命令行界面

CPU：Central Processing Unit，中央处理器，

ebXML：eBusiness XML，电子商务XML

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

EIP：Enterpise Information Portal，企业信息门户

ESB：Enterprise Service Bus，企业服务总线

ETL：Extract- Transform- Load，数据抽取、转换、装载

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

HIS：Hospital Informaton System，医院信息系统

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

I/O：Input/Output，即输入输出

ID：Identity，标识号

IHE：Integrating Healthcare Enterprise，医疗健康信息集成规范

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

ISDN：Integrated Service Digital NeTwork，综合业务数字网

Java：Sun公司推出的面向对象的编程语言

JMS：Java Message Service，Java消息服务

KVM：Keyboard Video Mouse，即多计算机切换器，

LED：Light Emitting Diode，发光二极管

LIS：Lab Information System，检验信息系统

LOINC：Logical Observation Identifiers Names and Codes，实验室结果和观察信息代码

NAS： Network Attached Storage, 网络附加存储

NFS：Network File System,网络文件系统

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

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

PKI：Public Key Infrastructure，公开密钥体系

POS：Point of Service，服务点

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

RIS：Radiology Information System，放射信息系统

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

SFP: Small Form-factor Pluggable transceiver，小封装可插拔收发器

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，

SNOMED：Systematized Nomenclature of Medicine，系统化医疗术语

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

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

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

URI：Unified Resource Identity，统一资源标识

VPN：Virtual Private Network，虚拟专用网络

XDS：Cross-Enterprise Document Sharing，跨医疗卫生机构的文档共享

XFP：10-Gigabit small Form-factor Pluggable transceiver,万兆以太网接口小封装可插拔收发器

XML：Extensible Markup Language，可扩展标识语言

4 省级人口健康综合管理平台框架和技术要求

4.1 总体框架

省级人口健康综合管理平台参见WS/T 448-2014，包括信息基础设施、信息资源中心、省级人口健康综合管理平台服务、基于省级人口健康综合管理平台的应用、标准规范、信息安全，如下图所示。

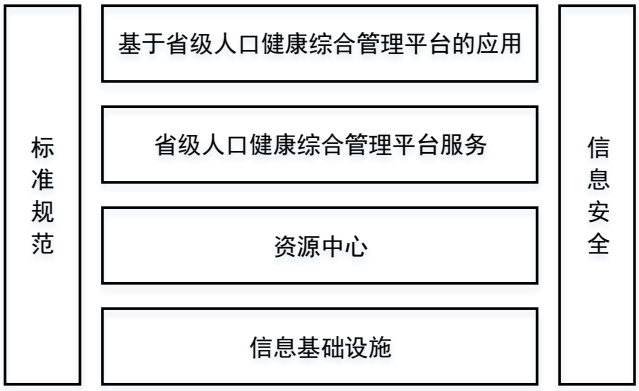

图1 省级人口健康综合管理平台总体框架

4.2 符合面向服务的体系结构的技术框架

省级人口健康综合管理平台采用面向服务的体系结构（SOA）的技术路线。在 SOA 体系结构中，服务即可以是传统的基于 Web Service 的服务，也可以是目前面向互联网的基于 REST 的轻量级服务。

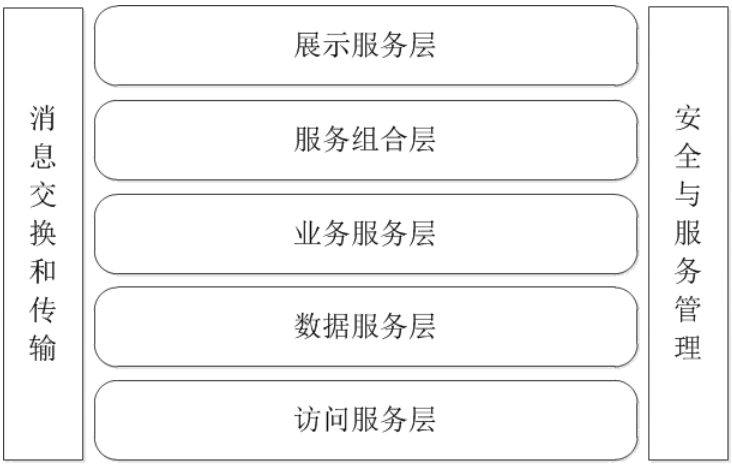

图2　面向服务的技术框架

a）　展现服务层

展现服务层定义企业信息门户（EIP）中可配置、可重用的门户组件（Portlets），用于支持门户应用的开发；以及人机交互组件、网页组件、报表组件实现对不同客户接入方式的支持，并提供丰富的客户端展现方式。在基于省级人口健康综合管理平台的应用中，健康档案浏览器、居民健康公众服务等主要在展现服务层体现。同时，随着大量移动终端设备的出现，移动客户端应用同样可以用于健康信息的展现。

b）　服务组合层

服务组合层通过对下层的访问服务、数据服务、业务服务的编排来实现，流程编排的规则在该层内定义，通过服务的编排组合就可以快速搭建出新的业务应用系统。在省级人口健康综合管理平台中，健康档案调阅服务、健康档案协同服务等服务主要在服务组合层体现。

c）　业务服务层

业务服务层定义那些可重用的业务处理过程，用于支持复合的业务处理需求。这层定义的业务处理过程服务可能是单个原子事务的无状态处理操作服务，也可能是多个业务应用或异步服务之间交互的有状态处理操作服务。业务服务层之上的开发者无需知道具体某项业务的逻辑处理过程。在省级人口健康综合管理平台中，注册服务、健康档案存储服务、健康档案管理服务等服务主要在业务服务层体现。

d）　数据服务层

数据服务层定义的服务支持把异构的、孤立的企业数据转变成集成的、双向的、可重复使用的信息资源。数据服务通过访问服务层以统一的方式访问企业的所有数据，数据服务层之上的开发者可以集中精力处理数据的加工问题，而不必关注访问不同来源的数据的实现细节。在省级人口健康综合管理平台中，健康档案整合服务、数据仓库等主要在数据服务层体现。

e）　访问服务层

访问服务层实现与底层数据资源、应用资源的通信功能，使用通用标准接口，定义整合企业信息资源（数据资源与应用资源）的各种访问服务，例如：不同类型的适配器以及专用的API等等。访问服务屏蔽了企业信息资源（现在的或未来的）的技术和实现方式，访问服务层之上的开发者无需知道数据的位置、类型以及应用程序的编程语言等。在省级人口健康综合管理平台中，区域卫生信息交换层主要在访问服务层体现。

f）　消息交换和传输

服务间的消息交换和消息传输贯穿的各个服务层。消息交换和传输可以采用企业服务总线ESB。服务间的消息交换需要基于通用的交换标准和行业的交换标准。消息传输层可以提供通用的传输协议支持，如HTTP、HTTPS、SMTP、JMS、FTP等。

g） 安全与服务管理

安全管理和服务管理贯穿各个服务层。在省级人口健康综合管理平台中，信息安全与隐私保护主要在安全与服务管理层体现。

服务安全管理支持认证和授权、不可否认和机密性、安全标准等。基于WS的服务的安全管理遵循WS服务规范中WS-Security规范，其他形式的服务也需要提供安全保障

服务管理包括服务注册、服务发现、服务监控、服务治理等多方面的内容，本规范暂不对这些功能提出具体要求。

4.3 指导原则

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 的有关指引；
b） 在选择 SOA 技术标准规范时，应重点定义“服务接口”和消息协议标准或规范，对服务内部功能实现所采用的技术标准规范可不加限制；
c） 凡与 SOA 重用性密切相关的组件，如服务接口，必须采用成熟的技术标准规范；
d） 确保在省级人口健康综合管理平台上的业务数据是正确的，符合技术规范的要求。
e） 省级人口健康综合管理平台的数据采集采用的文档，遵循《卫生信息共享文档规范》提出的要求和版本控制。
f） 对还没有最后定案的事实标准或规范，作为可选技术参考使用。

5 省级人口健康综合管理平台参考模型架构

5.1 平台技术架构

本规范中的平台技术架构在《基于健康档案的区域卫生信息平台技术规范》的基础上，对平台组件构成做了进一步的完善和扩展。如图3所示：

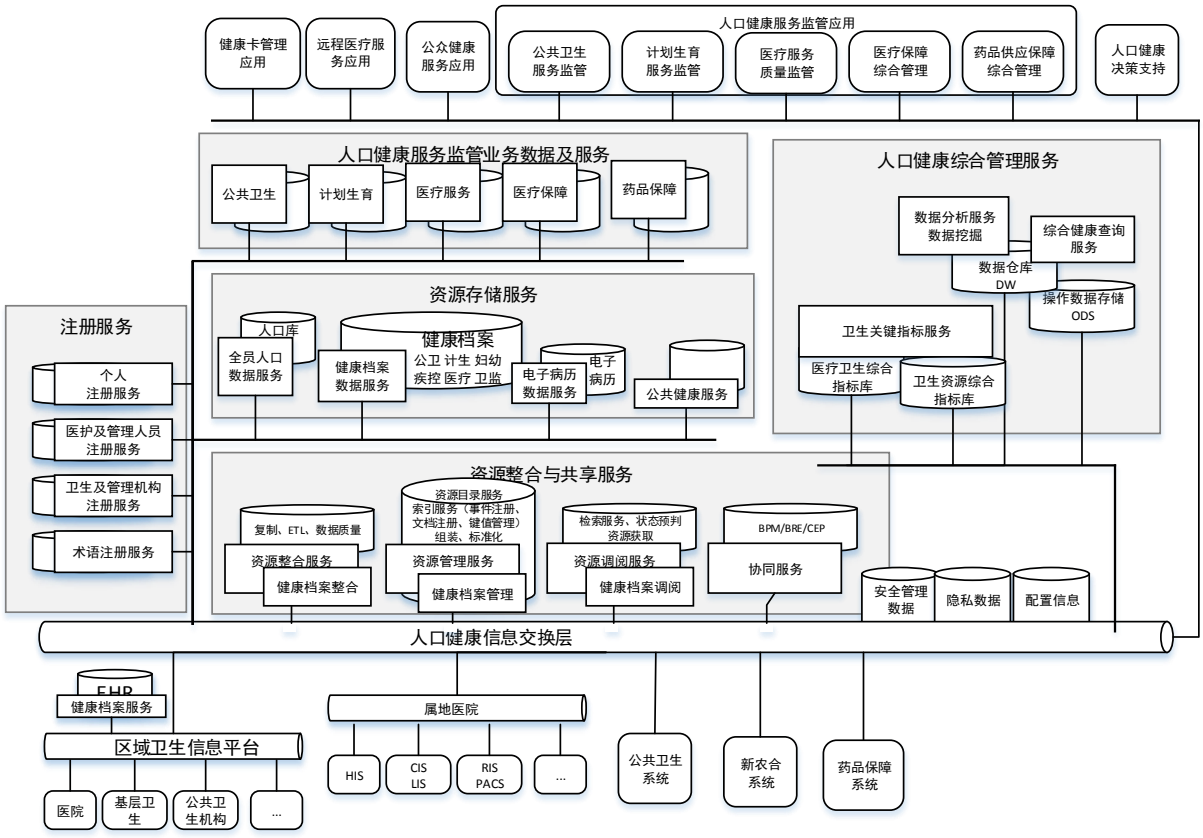

图3　省级人口健康综合管理平台技术架构

5.2　平台技术架构说明

5.2.1　注册服务功能

5.2.1.1　服务功能概述

提供对个人、医疗卫生人员、医疗卫生机构、术语等基础共享信息的注册，提供唯一的标识号，实现在省域范围内的信息识别。

5.2.1.2　个人注册服务功能

个人注册服务是在一定区域管辖范围内，用于安全地保存和维护个人的健康标识号、基本信息，提供给省级人口健康综合管理平台其他组件及POS应用所使用，并可为医疗就诊及公共卫生相关的业务系统提供人员身份识别功能的服务组件。个人注册服务形成一个个人注册库：

- 其一，它是唯一的个人基本信息权威信息来源，用于医疗卫生信息系统确认一个人是某个居民或患者。
- 其二，解决在跨越多个系统时居民身份唯一性识别的问题。

个人注册服务由医院、基层医疗卫生机构和公共卫生机构来使用，完成居民身份的注册。

个人注册服务应支持多种电子化的身份识别手段，包括居民健康卡、社会保障卡、第二代居民身份证等。

5.2.1.3 医疗卫生人员注册服务功能

医疗卫生人员注册库，是一个单一的目录服务，为本区域内所有卫生管理机构的医疗服务提供者，包括全科医生、专科医生、护士、实验室医师、医学影像专业人员、疾病预防控制专业人员、妇幼保健人员及其他从事与居民健康服务相关的从业人员，系统为每一位医疗卫生人员分配一个唯一的标识，并提供给平台以及与平台交互的系统和用户所使用。

5.2.1.4 机构注册服务功能

通过建立机构注册库，提供本区域内所有与健康档案及综合卫生管理相关的机构的综合目录，相关的机构包括卫生行政机构、二三级医院、基层医疗卫生机构、疾病预防控制中心、卫生监督所、妇幼保健所等。系统为每个机构分配唯一的标识，可以解决居民所获取的医疗卫生服务场所唯一性识别问题，从而保证在维护居民健康信息的不同系统中使用统一的规范化的标识符，同时也满足省级人口健康综合管理平台层与下属机构服务点层的互联互通要求。

5.2.1.5 行政区域注册

对地（地级市、州、盟）、县（县级市、旗、区）、乡（镇、街道、苏木、林区）、行政村（社区）各政的行政机构及归属进行管注册管理。维护每次变动的年份、名称、所辖情况变化。实现不同年份的健康档案具有历史的行政归属。

5.2.1.6 术语注册服务功能

建立术语注册库，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。术语可由平台管理者进行注册、更新维护。

5.2.2 资源整合与共享服务功能

5.2.2.1 服务功能概述

提供对包括健康档案与电子病历共享文档在内的相关信息的资源整合、资源管理、资源调阅及业务协同服务。

5.2.2.2 资源整合功能

提供健康档案文档与其它资源整合服务，支持数据资源的批量上传和个案数据实时上传。包括以下功能：

——复制功能：在现有的省级人口健康综合管理平台内的系统或数据库之间提供数据复制功能；在本规范中暂不规定复制功能的服务和接口。

——ETL 功能：数据仓库服务从不同的存储库中抽取和插入数据，经过抽取、转换和装载等加工处理后，提供生成省级人口健康综合管理平台范围内使用的各种数据资源分析利用资源；在本规范中暂不规定与 ETL 相关的服务和接口。

——数据质量控制功能：用于跟踪和监控省级人口健康综合管理平台里的数据质量。

本规范中暂不规定与数据质量控制相关服务和接口。

5.2.2.3 资源管理功能

提供资源注册、事件注册、索引服务、组装服务、标准化服务等资源相关的管理服务功能。包括：

——资源注册功能：

资源注册包括健康档案与电子病历文档资源及其它资源的注册，资源注册服务根据资源提供者提交的资源元数据，维护文档及其它数据资源的注册元数据，包括在资源库中存储的地址。资源获取用可根据文档用户的特定查询条件返回文档（集）。

——事件注册功能

为实现区域内医疗卫生信息系统之间对健康档案信息的共享和交换，需要在区域内部以居民或患者为单位，对居民获得的卫生服务活动的事件信息进行注册。

事件注册本质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，实际操作时，应该提取文档中与事件相关的元数据进行注册，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。

——索引服务功能

索引服务全面掌握省级人口健康综合管理平台所有关于居民的医疗卫生服务事件信息，包括居民何时、何地、接受过何种医疗卫生服务，并产生了哪些文档。索引服务主要记录两大类的信息，一是医疗卫生事件信息，另一为文档目录信息。

省级人口健康综合管理平台用户在被授权的情况下，可以通过索引服务从POS系统查看某居民的健康事件信息，以及事件信息所涉及的文档目录及摘要信息。再结合健康档案存储服务可以实现文档信息的即时展示，使用户更多的了解居民（患者）既往的健康情况。

——组装服务功能

组装服务通过调用不同的平台组件生成多个健康档案数据的结果集，并把这些结果集组合成一定输出格式。

——标准化服务功能

标准化服务把特定的输入串修改成符合标准化的编码串。数据的格式和实质含义都可以转换。

5.2.2.4 资源调阅服务功能

提供包括健康档案资源在内的资源检索服务、资源状态预判服务、资源获取服务：

——资源检索服务

通过资源检索获取符合条件的注册资源的目录、或健康档案（电子病历）索引；

——资源状态预判服务

提供对给定资源存储状态的预判，以进一步获取资源。

——资源获取服务功能

资源获取服务提供对给定资源的实际访问，获取包括健康档案（电子病历）文档、文档集在内资源的，获取的数据的检索和访问服务。

5.2.2.5 协同服务

省级人口健康综合管理平台应通过企业服务总线、业务流程管理、业务规则管理、事件管理等机制，实现医疗卫生业务协同服务。

协同服务应支撑跨地市服务、医防融合、三医联动、与其他委办、与互联网等的协同。协同服务主要服务。

5.2.3 资源存储服务功能

5.2.3.1 服务功能概述

提供全员人口资源库、健康档案资库、电子病历资源库以及公众健康信息的存储，并提供相应的数据共享服务功能。

5.2.3.2 全员人口存储服务

建立在全口人员库基础上的数据服务。全员人口库主要提供基本人口信息、流动人口信息、计划生育人口信息。

5.2.3.3 健康档案存储服务

健康档案存储服务是建立在一系列健康档案存储库基础上的数据服务。根据健康档案信息的分类，健康档案存储服务可包括七个存储库：个人基本信息存储库、主要疾病和健康问题摘要存储库、儿童保健存储库、妇女保健存储库、疾病控制存储库、疾病管理存储库以及医疗服务存储库。

5.2.3.4 电子病历存储服务

电子病历存储服务是建立在一系列电子病历存储库基础上的数据服务。根据电子病历信息的分类，电子病历存储存储库应提供对以下内容的电子病历分类与存储：病历概要、门（急）诊病历、门（急）诊处方、检查与检验报告、门急诊治疗处置记录、助产记录、门（急）诊助理记录、知情告知信息、住院病案首页、住院志、住院病程记录、住院医嘱、出院记录。电子病历存储库应建立与健康档案存储库的有机关联，实现通过健康档案访问相应电子病历的功能。

5.2.3.5 公众健康存储服务

提供公众健康所需的各类卫生信息，可通过网站、手机APP等终端发布。

5.2.3.6 其它资源存储服务

其它存储服务提供对外可扩展的存储服务服务功能。其它资源存储库提供包括其它领域接入数据存储、对外共享数据存储。对外提供的其它领域可能包括人力资源及社会保障、食品药品监管、公安、民政、全国组织机构管理等。

5.2.4 人口健康服务监管业务数据及服务

5.2.4.1 服务功能概述

提供对人口健康不同领域的服务监管业务数据及服务；这些数据及服务宜包括公共卫生、医疗服务、医疗保障、药品保障、计划生育等。

5.2.4.2 公共卫生

包括传染病动态监测、慢性病监测、重点职业病防治监测、食品安全风险监测评估、妇幼健康管理国家免疫规划、严重精神病障碍信息管理、卫生应急指挥、综合监督管理、中医药艾滋病管理。

5.2.4.3 医疗服务

包括预约诊疗监管与服务、远程医疗监管与服务、中西医电子病历共享、中医药管理业务、中医药服务业务、中医药资源信息服务。

5.2.4.4 医疗保障

包括新农合跨省费用核查、新农合异地结算、新农合运行监管。

5.2.4.5 药品保障

包括药品供应保障、基本药物制度运行监测评价。

5.2.4.6 计划生育

包括计划生育服务。

5.2.5 人口健康综合管理服务

5.2.5.1 服务功能概述

人口健康综合管理服务提供跨领域的综合管理，应包括卫生关键指标的管理、综合健康查询服务以及基于操作数据存储（ODS）或数据仓库数据集市的数据分析、数据挖掘服务。

5.2.5.2 卫生关键指标服务

卫生关键指标应包括综合卫生统计指标：健康影响因素、主要健康问题、妇幼保健、疾病预防控制、卫生监督、计划生育、资源管理。卫生关键指标服务应建立综合卫生统计指标库，提供对医疗卫生业务服务及资源管理各个业务领域的关键指标管理。

医疗卫生服务方面主要包括以下指标信息：

——居民健康状况及影响因素指标管理信息：包括居民健康状况管理信息、健康影响因素管理信息

——公共卫生服务统计管理指标管理信息：包括疾病控制、妇幼保健、卫生监督、医疗服务利用、医疗服务效率、医疗服务统计管理指标、医疗质量与安全、病人费用等统计管理指标；

——医疗保障（新农合）统计管理指标：包括基本医保覆盖、基本医保筹资等统计管理指标；

——卫生资源统计管理指标：包括卫生设施、卫生人力资源、卫生经费等统计管理指标；

——医品与材料供应保障：包括药品供应保障、卫生材料供应。

卫生资源管理方面统计指标包括：

——卫生机构与设施管理信息：包括卫生机构基本信息库、卫生服务设施库；

——卫生经费管理信息：包括经费筹集管理信息、经费使用管理信息。

5.2.5.3 综合健康查询服务

提供对跨领域的综合健康查询。

5.2.5.4 数据分析数据挖掘

可建立操作数据存储（ODS）或数据仓库、数据集市，通过联机数据分析、数据挖掘等技术手段，提供对给定主题的数据分析和知识发现。同时宜建立知识库，提供对知识的存储与查询。为使用者提供管理辅助决策和临床辅助决策支持。

在本规范中暂不规定与操作数据存储、数据仓库相关服务和接口。

5.2.6 信息安全与隐私保护

省级人口健康综合管理平台应该通过提供身份认证、用户管理和权限控制、审计追踪、加密服务、知情同意、匿名服务等手段保证信息安全和隐私保护。

5.2.7 公众省级人口健康信息交换层

省级人口健康信息交换层应采用企业服务总线等符合 SOA 技术路线的产品来搭建。省级人口健康信息交换层是省级人口健康综合管理平台与所有 POS 应用、公众健康服务、外部用户访问的数据访问总线，为任何授权应用服务访问 EHRs 提供统一网关。

在本规范中暂不规定与省级人口健康信息交换层相关的服务和接口。

5.2.8 人口健康服务应用

5.2.8.1 公众健康服务应用

省级人口健康综合管理平台可通过门户网站、电子邮件、短信、移动App、健康物联网、可穿戴设备、社交网络等多种方式为居民提供电子化的健康服务应用。这些应用包括是预约挂号、健康门户、政策公示、就诊评价、健康咨询等。

在本规范中暂不规定与数据仓库相关服务和接口。

5.2.8.2 居民健康卡服务应用

应用平台所提供的服务，通过居民健康卡识别、定位居民健康信息。

5.2.8.3 远程医疗服务应用

应用平台的所提供的服务，实现跨机构、跨地区的医疗服务活动，宜包括以检查诊断为目的的远程医疗诊断、以咨询会诊为目的的远程医疗会诊、以教学培训为目的的远程医疗教育和以家庭病床为目的的远程病床监护等服务应用。

5.2.8.4 人口健康服务监管应用

应用人口健康服务监管数据及服务，以及平台其它相关服务，提供对公共卫生、计划生育、医疗服务、医疗保障、药品供应保障等方面的监督与管理应用，同时可通过人口健康综合服务，提供各个业务与管理领域的决策支持。包括：

——公共卫生服务监管：提供对妇幼保健、疾病预防控制、卫生监督、卫生应急指标等公共卫生相关的服务监管。

——计划生育服务监管：提供对人口与计划生育相关的服务监管。

——医疗质量服务监管：可提供包括医疗事故、院感、用药、临床路径、医疗服务记录等方面的服务监管。

——医疗保障（新农合）服务监管：提供对新农合参与及受益情况、医疗服务利用和医药费用控制、参合人员疾病负担情况、服务评价、基金筹集与分配等方面的监管。

——药品供应保障服务监管：提供对药品供应商及药品采购、验收、运输、储存、销售、使用过程的服务监管。

——人口健康决策支持：应用人口健康综合管理服务提供的卫生关键提标服务、综合卫生

6 平台功能和交易规范

6.1 注册服务

6.1.1 个人注册服务

6.1.1.1 服务概述

个人注册服务参见WS/T 448-2014平台功能和交易规范。

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

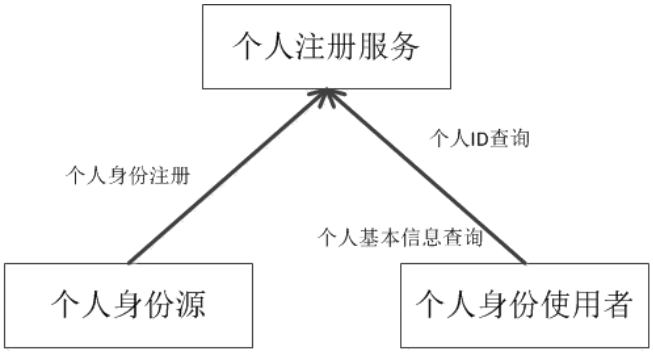

图4　个人注册服务角色交易图

个人注册服务组件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。

6.1.1.2　个人身份注册服务

个人身份注册，即为个人身份提交，是将多个域来源的同一个人的身份信息进行新增、修订和合并。个人身份注册为不同来源的同一个人的身份信息能够被识别奠定基础。

角色和交易

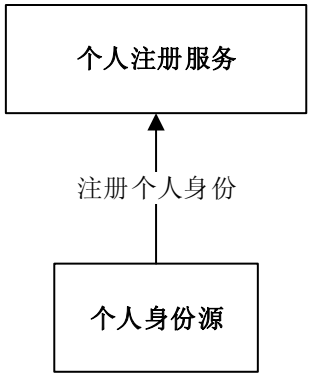

图5　个人身份注册角色交易图

个人身份注册服务涉及两个角色，个人身份源和个人注册服务组件。个人身份源向个人注册服务组件提交本域中的个人唯一身份信息。

角色交易选择

表1　个人身份注册角色-交易关系表

角色	交易	选择
个人身份源	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	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）

交易流程

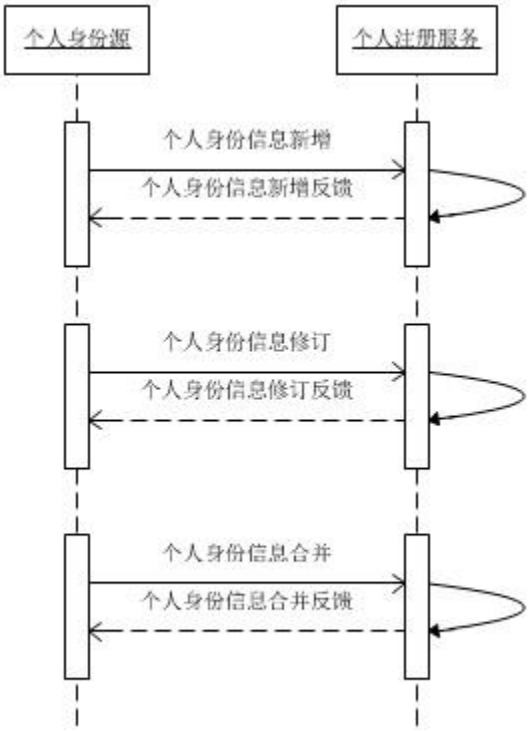

图6　个人身份注册时序图

- 个人身份源向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；
- 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。

交易消息

参考附录 A：个人身份信息新增、个人身份信息修订、个人身份信息合并。

6.1.1.3　个人 ID 查询服务

个人ID查询指通过一个已知个人ID来获取其它域的相关个人ID。

角色和交易

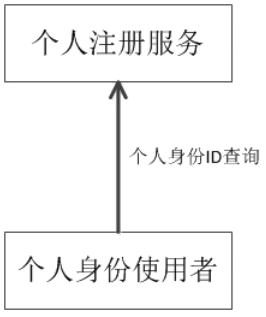

图7　个人 ID 查询角色交易图

个人ID查询涉及两个角色，个人身份使用者，个人注册服务组件。个人ID使用者向个人注册服务组件提交个人ID查询。

角色交易选择

表2　个人 ID 查询角色-交易关系表

角色	交易	选择
个人身份使用者	个人 ID 查询	必须（R）
个人注册服务组件	个人 ID 查询反馈	必须（R）

交易流程

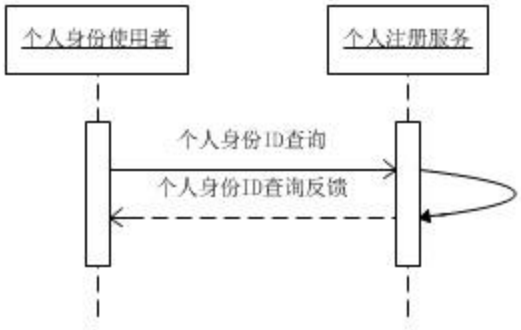

图8　个人 ID 查询时序图

- 个人身份使用者向个人注册服务组件提交个人身份查询；
- 个人注册服务组件返回相关个人身份。

交易消息

参见附录 A：个人身份 ID 查询、个人身份 ID 查询反馈。

6.1.1.4　个人基本信息查询服务

个人基本信息查询是根据查询条件，返回符合条件的个人基本信息。

角色和交易

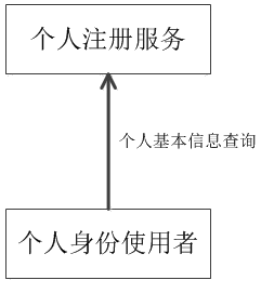

图9　个人基本信息查询角色交易图

个人基本信息查询涉及两个角色，个人基本信息使用者，个人注册服务组件。个人基本信息使用者向个人基本信息注册服务注册提交个人基本信息查询。

角色交易选择

表3　个人基本信息查询角色-交易关系表

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）
个人注册服务组件	个人基本信息查询	必须（R）

交易流程

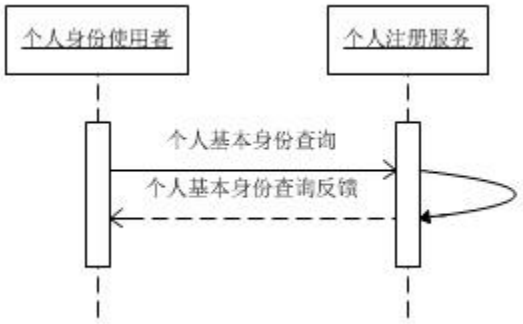

图10　个人基本信息查询时序图

- 个人基本信息使用者向个人注册服务组件提交个人基本信息查询；
- 个人注册服务组件返回个人基本信息。

6.1.2　医疗卫生人员注册服务

服务概述

医疗卫生人员注册服务参见WS/T 448-2014平台功能和交易规范。

医疗卫生人员注册，为本区域内所有医疗卫生机构的医疗服务提供者，包括全科医生、专科医生、护士、实验室医师、医学影像专业人员、疾病预防控制专业人员、妇幼保健人员及其他从事与居民健康服务相关的从业人员，分配一个唯一的标识，并提供给平台以及与平台交互的系统和用户所使用。

角色和交易

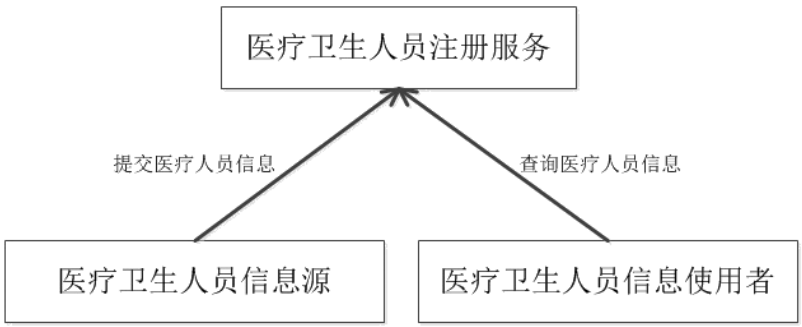

图11　医疗卫生人员注册角色交易图

表4　医疗卫生人员注册角色-交易关系表

角色	交易	可选性
医疗卫生人员信息源	提交医疗卫生人员信息	必须(R)
医疗卫生人员信息使用者	查询医疗卫生人员信息	必须(R)
医疗卫生人员注册服务	提交医疗卫生人员信息	必须(R)
	查询医疗卫生人员信息	

角色交易选择

表5　医疗卫生人员注册角色选择

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

交易流程

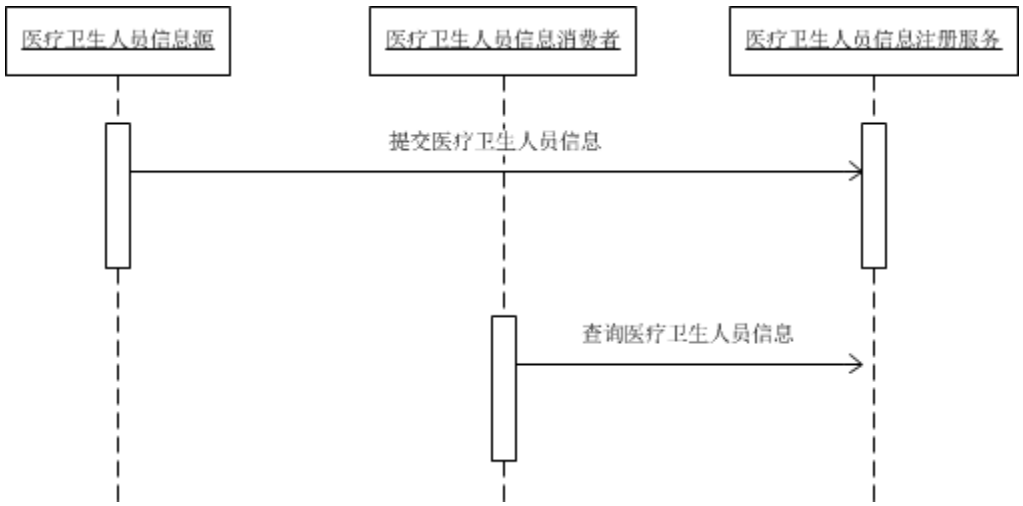

图12　医疗卫生人员注册时序图

- 区域内医疗卫生机构系统（如医院 HIS 系统）作为医疗卫生人员信息源，向省级人口健康综合管理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；
- 区域内医疗卫生机构系统（医生工作站）在某个跨机构的业务中，查询相关医疗卫生人员的信息。例如在调阅个人健康档案时，检验报告中有报告创建者信息，医生工作站系统作为医疗卫生人员信息使用者，查询医疗卫生人员信息，并在报告中显示报告创建者的可显示的名字等信息。

6.1.3　机构注册服务

服务概述

通过建立机构注册服务，提供本区域内所有机构的综合目录，相关的机构包括二三级医院、基层医疗卫生机构、疾病预防控制中心、卫生监督所、妇幼保健所以及卫生行政管理机构等。系统为每个机构分配唯一的标识，可以解决居民所获取的医疗卫生服务场所唯一性识别问题，从而保证在维护居民健康信息的不同系统中使用统一规范的标识符，同时也满足省级人口健康综合管理平台层与下属医疗卫生机构服务点层的互联互通要求。

角色和交易

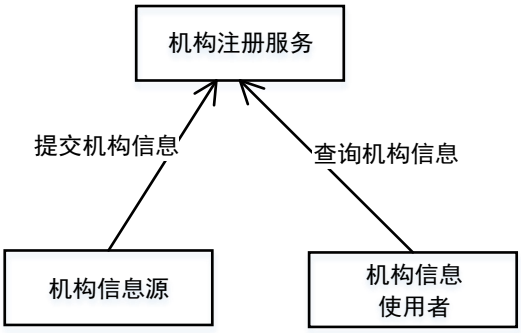

图13　机构注册角色交易图

表6　机构注册角色-交易矩阵

角色	交易	可选性
机构信息源	提交机构信息	必须（R）
机构信息使用者	查询机构信息	必须（R）
机构注册服务	提交机构信息	必须（R）
	查询机构信息	

角色交易选择

表7　机构注册角色选择

角色	选择
机构信息源	必须（R）
机构信息使用者	必须（R）
机构注册服务	必须（R）

交易流程

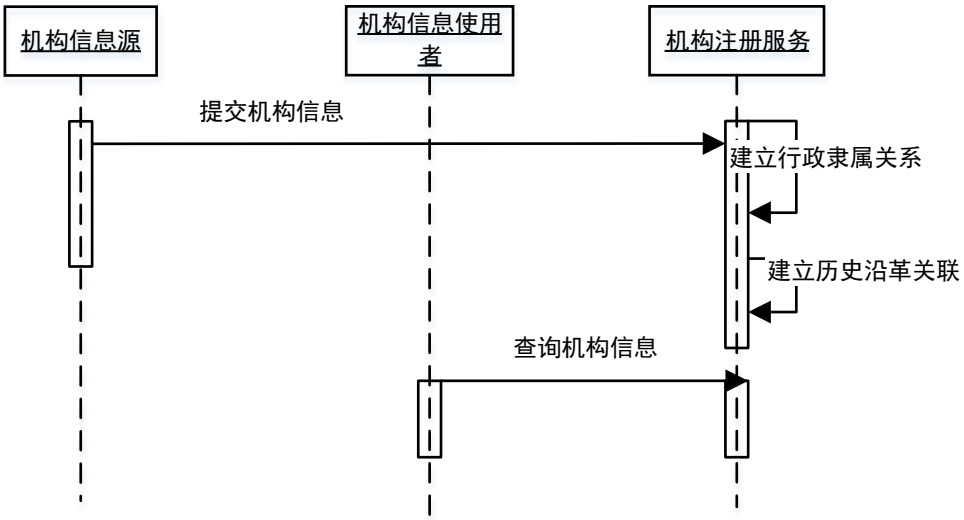

图14　机构注册时序图

- 区域内综合管理系统作为机构信息源，向省级人口健康综合管理平台中机构注册服务提交区域内机构信息；
- 区域内医疗卫生系统（如医生工作站）在某个跨机构的业务中，查询相关机构的信息。例如在调阅个人健康档案时，检验报告中有报告创建者信息，医生工作站系统作为机构信息使用者，查询医疗卫生机构信息，并在报告中显示报告创建机构的可显示的名字等信息。

6.1.4　行政区域注册服务

服务概述

通过建立从地市级到村社区级行政注册服务，反应不同时期区域的变化与传承，支持历史健康档案与区域的映射。行政区域包括省级、地市级、县区级、乡镇级、村级、社区级的。系统为每个区域分配唯一的标识,可解决行政区域的唯一性识别问题,并对区域的历史沿革建立索引、对所属区域建立关联，实现区域历史的变化认定、以及区域的从属关系认定。从而提供在维护居民健康信息的不同系统中使用统一规范的区域标识符。

角色和交易

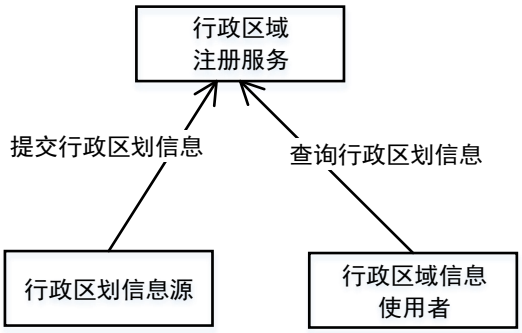

图15　行政区域注册角色交易图

表8　行政区域注册角色-交易矩阵

角色	交易	可选性
行政区划信息源	提交行政区划信息	必须（R）
行政区域信息使用者	查询行政区域基本信息	必须（R）
	查询历史行政区划基本信息	必须（R）
	查询所辖行政区划信息	
行政区域注册服务	提交医疗卫生机构信息	必须（R）
	查询医疗卫生机构信息	
	查询历史行政区划基本信息	
	查询所辖行政区划信息	

角色交易选择

表9　医疗卫生机构注册角色选择

角色	选择
行政区划信息源	必须（R）
行政区域信息使用者	必须（R）
行政区域注册服务	必须（R）

交易流程

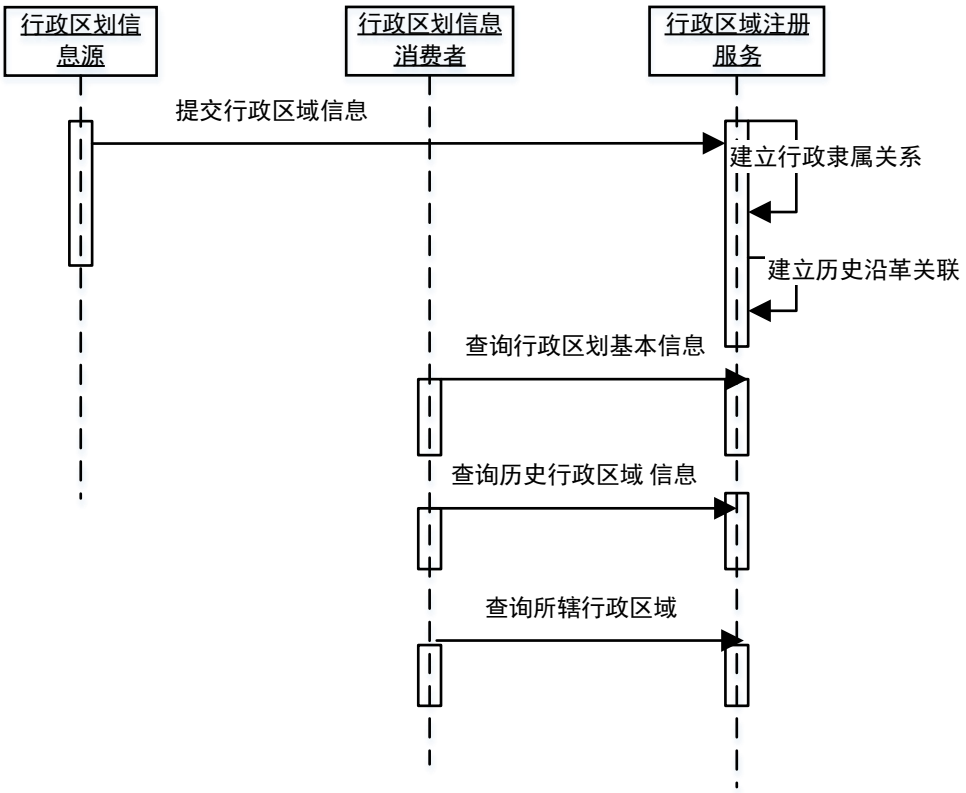

图16　医疗卫生机构注册时序图

- 平台管理作为行政区域信息源，向省级人口健康综合管理平台行政区域注册服务提交区域信息，信息包括区划编码、上级区域、关联历史区域、区域名称等；
- 行政区域信息用户可以查询行政区域基本信息、历史行政区域信息（有效期起止年份）。查询所辖行政区域等。

6.1.5　术语注册服务

6.1.5.1　服务概述

术语注册服务参见WS/T 448-2014平台功能和交易规范。

6.1.5.2　术语模型

标准化术语体系是整个平台体系内部或与外部系统在信息表达和语义互操作时的关键性基础设施。标准化术语体系，须包含以下几部分：

1）　省级人口健康综合管理平台范围内各层面各类型数据（或信息）中，代码化的信息标准表达模型；
2）　省级人口健康综合管理平台范围内各层面各类型数据（或信息）中，术语类的信息标准表达模型；
3）　省级人口健康综合管理平台引入的所有代码、术语，及其在平台中的具体存在和表达形态；
4）　代码、术语之间若有内在关联，则用于表达其关系的数据模型也需明确提出。

6.1.5.3　注册、更新及版本管理

角色和交易

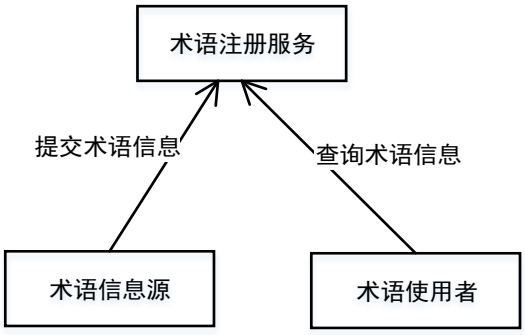

图17　术语注册角色交易图

术语注册活动主要有三类角色参与，术语注册服务组件、术语消息源与术语使用者。

角色交易选择

表10　术语注册角色的选择

角色	交易	选择
术语注册服务	术语提交	必须（R）
	术语查询	必须（R）
术语消息源	术语提交	必须（R）
术语使用者	术语查询	必须（R）

交易流程

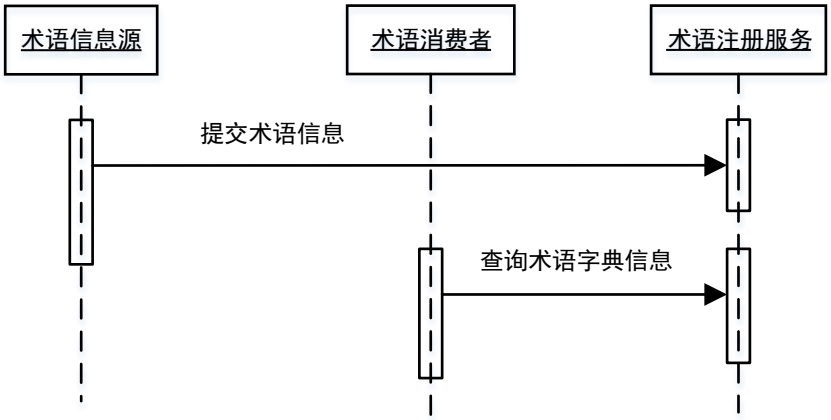

图18　术语注册时序图

- 术语提供者提交其原始术语到术语注册服务组件；
- 术语注册服务组件校验并进行相应的注册、更新、版本变更等行为。

6.1.5.4　术语代码映射

角色和交易

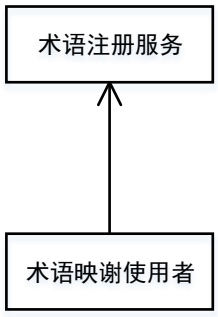

图19　术语代码映射角色交易图

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

角色交易选择

表11　术语代码映射角色的选择

角色	交易	选择
术语注册服务	术语代码映射检索	必须（R）
术语映射使用者	术语代码映射检索	必须（R）

交易流程

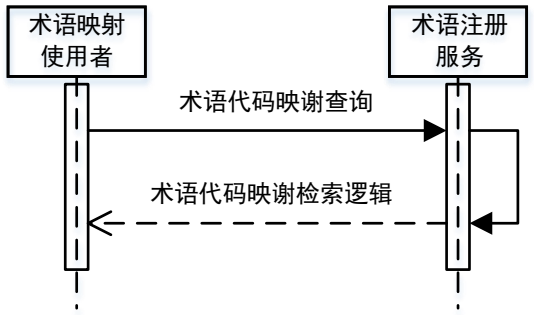

图20　术语代码映射时序图

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

6.2 信息资源[EHR]整合与共享服务

6.2.1 信息资源[EHR]整合服务

信息资源[EHR]整合服务参见 WS/T 448-2014 平台功能和交易规范健康档案整合服务。

信息资源[EHR]整合服务提供对信息资源[EHR]的采集，包括个案实时的数据采集和批量数据采集。该服务同样适用于电子病历整合服务以及综合管理数据整合服务。

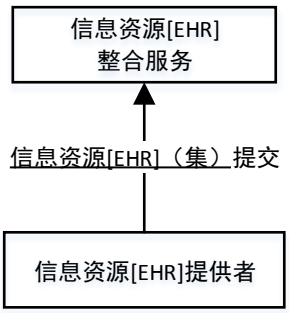

图21 健康档案整合服务角色交易图

6.2.1.1 个案实时的数据采集（XML）

个案实时的数据采集是通过Web Service将XML格式的信息资源[EHR]进行实时采集。

角色和交易

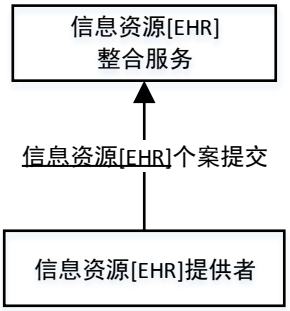

图22 健康档案个案实时提交角色交易图

个案实时的数据采集涉及两个角色，一是信息资源[EHR]提供者，二是信息资源[EHR]整合服务。健信息资源[EHR]提供者向信息资源[EHR]整合服务实时提交信息资源[EHR]个案信息。

角色交易选择

表12 健康档案个案实时提交角色的选择

角色	交易	选择
信息资源[EHR]提供者	个案实时提交	必须（R）
信息资源[EHR]整合服务	个案实时提交	必须（R）

交易流程

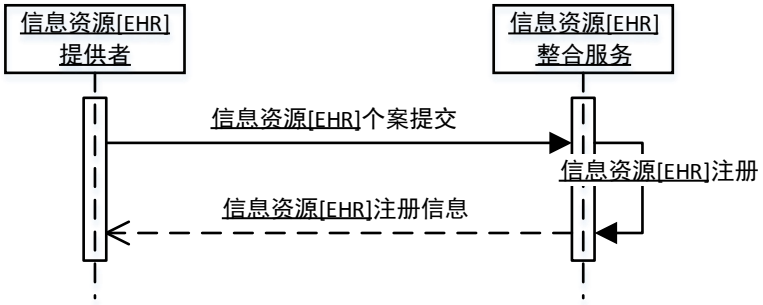

图23　信息资源[EHR]个案实时提交时序图

- 信息资源[EHR]提供者向信息资源[EHR]整合服务实时提交个案；
- 信息资源[EHR]提供者对信息资源[EHR]进行处理。

6.2.1.2　批量数据采集

批量数据采集是非实时大批量数据的采集方式的，一般时间延时在1天之内。

角色和交易

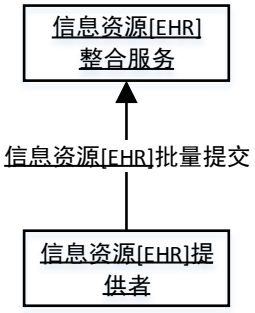

图24　信息资源[EHR]批量数据采集角色交易图

个案实时的数据采集涉及两个角色，一是信息资源[EHR]提供者，二是信息资源[EHR]整合服务。信息资源[EHR]提供者向信息资源[EHR]整合服务非实时批量提交健康档案。

角色交易选择

表13　信息资源[EHR]批量数据采集角色的选择

角色	交易	选择
信息资源[EHR]提供者	批量提交	必须（R）
信息资源[EHR]整合服务	批量提交	必须（R）

交易流程

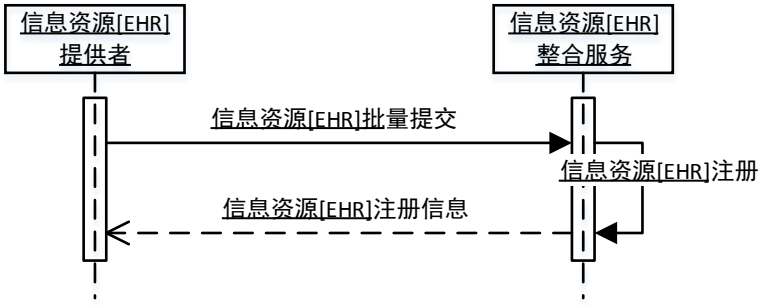

图25　健康档案批量数据采集时序图

- 信息资源[EHR]提供者向信息资源[EHR]整合服务批量提交信息资源[EHR]；
- 信息资源[EHR]整合服务对信息资源[EHR]数据进行注册处理。并返回注册信息。

6.2.1.3　基于 XDS 的数据采集

在个案实时的数据采集中，可以按照符合XDS规范的方式提交文档。
具体交易请参见6.3健康档案存储服务。

6.2.2　资源管理服务

6.2.2.1　资源管理

参见WS/T 448-2014平台功能和交易规范健康档案服务。

资源访问审计

角色和交易

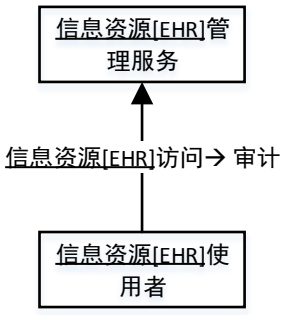

图26　健康档案访问审计角色交易图

信息资源[EHR]访问审计活动发生于任何信息资源[EHR]的读、写操作中，主要由两类角色参与，信息资源[EHR]使用者与信息资源[EHR]管理服务组件，信息资源[EHR]使用者泛指所有接触到某份信息资源[EHR]的对象（包括外部系统、内部子系统、平台自身等），信息资源[EHR]访问交易泛指所有与信息资源[EHR]的接触动作，如修改、更新、调阅等等。

角色的选择

表14　信息资源[EHR]访问审计角色选择表

角色	交易	选择
信息资源[EHR]管理服务	信息资源[EHR]访问审计	必须（R）
信息资源[EHR]使用者	信息资源[EHR]访问审计	必须（R）

交易流程

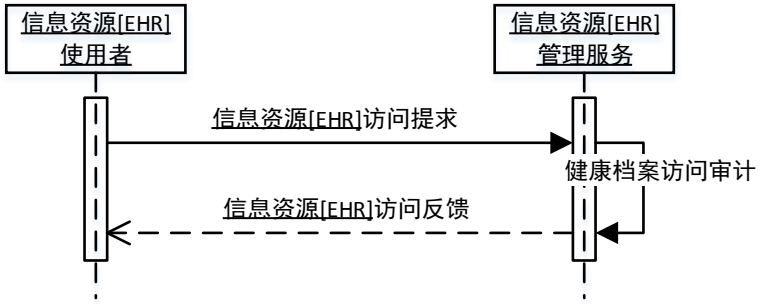

图27　信息资源[EHR]访问审计时序图

- 信息资源[EHR]访问者向信息资源[EHR]管理者发起各种形式的访问请求；
- 信息资源[EHR]管理者对该次访问动作进行行为审计。

6.2.2.2　文档注册

参见WS/T 448-2014平台功能和交易规范文档注册。

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。文档注册角色需要根据文档用户的特定查询条件返回文档（集）。文档注册时它会要求一些特定的卫生服务信息的隐私技术策略。

具体交易请参见 6.3 健康档案存储服务。

6.2.2.3　组装服务

参见WS/T 448-2014平台功能和交易规范组装服务。

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一起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。

a) 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。

b) 信息资源[EHR]摘要组装服务

信息资源[EHR]摘要组装的服务。EHR摘要包括不限于：

- EHR 摘要：免疫接种史、过敏史、分娩史、慢病史等。
- 慢病跟踪曲线图。
- 最近就诊记录。

c) 信息资源[EHR]目录组装服务

按照多种维度和多层级来形成信息资源[EHR]目录。EHR多种维度包括：“健康事件”、“生命周期”、“健康问题”和“干预措施”。此外也可以基于医药卫生机构注册和医药卫生人员注册，按照机构、按照医务人员等维度来展示。

d) EHR 首页组装服务

把居民基本信息、EHR目录和EHR摘要等内容组装成EHR首页的服务。可在个人基本信息组装服务、EHR摘要组装服务和EHR目录组装服务的基础上封装。

6.2.2.4 标准化服务

参见WS/T 448-2014平台功能和交易规范标准化服务。

这些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。典型地，这个服务常用于应用标准，把特定的输入串修改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化。可以基于术语字典注册开发。

具体交易参见6.1.4.3代码映射。

6.2.3 信息资源[EHR]调阅服务

信息资源[EHR]浏览服务用于处理省级人口健康综合管理平台内与数据定位和管理相关的复杂任务。该服务包括相关的组装服务、标准化服务以及数据访问服务。信息资源[EHR]服务负责分析来自外部资源的请求，响应外部医疗卫生服务点的检索、汇聚和返回数据，也可以反向地存这些数据到存储库中。

6.2.3.1 信息资源[EHR]检索服务

参见WS/T 448-2014平台功能和交易规范健康档案检索服务。

信息资源[EHR]检索服务，输入信息资源[EHR]检索条件，输出信息资源[EHR]索引信息。

角色和交易

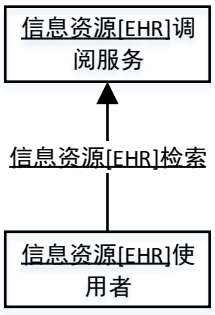

图28 EHR 调阅目录角色交易图

EHR调阅消费者请求调阅目录服务，EHR调阅服务接收调阅请求，EHR调阅服务返回结构化数据。

交易的选择

表15 EHR 调阅目录角色交易表

角色	交易	选择
EHR 调阅服务	调阅目录服务	必须（R）
EHR 调阅消费者	调阅目录服务反馈	必须（R）

交易流程

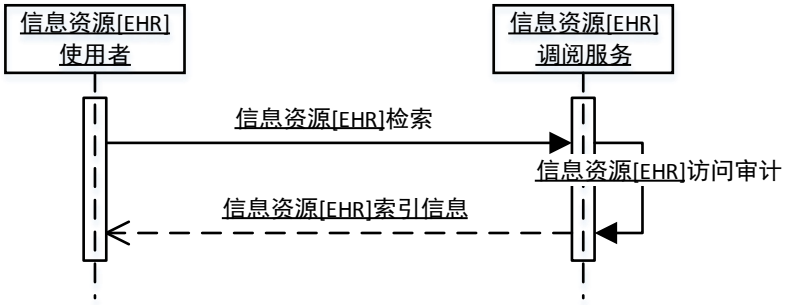

图29　EHR 调阅目录时序图

调阅目录服务由EHR调阅消费者发起，其请求中应包含个人标识信息，EHR调阅服务根据提供的个人标识信息返回按时间排序的结构化数据。EHR调阅消费者可根据获取的结构化数据任意组织展示形式。

6.2.3.2　资源状态查询服务

参见WS/T 448-2014平台功能和交易规范健康档案预判服务。

角色和交易

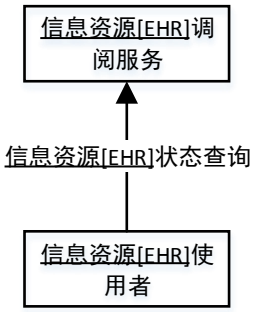

图30　调阅预判角色交易图

- 信息资源[EHR]调阅消费者发送信息资源[EHR]状态查询请求；
- 信息资源[EHR]调阅服务判断是否存在指定信息资源[EHR]数据，并返回给信息资源[EHR]使用者。

交易的选择

表16　信息资源[EHR]状态查询角色交易表

角色	交易	选择
信息资源[EHR]调阅服务	状态查询	可选（O）
信息资源[EHR]使用者	状态查询	可选（O）

交易流程

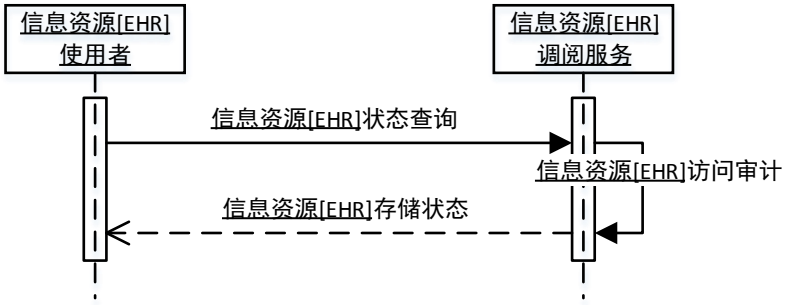

图31　状态查询时序图

状态查询交易由信息资源[EHR]使用者发起，信息资源[EHR]调阅服务接收到请求后，判断是否存在居民的EHR数据，并把存储状态回给信息资源[EHR]使用者。

6.2.3.3　信息资源[EHR]获取服务

参见WS/T 448-2014平台功能和交易规范健康档案调阅服务。

角色和交易

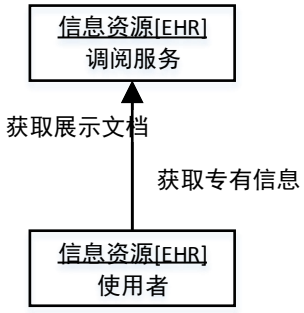

图32　调阅展示角色交易图

- EHR 调阅消费者发起获取专有展示文档及获取调阅展示文档交易；
- EHR 调阅服务接收获取专有展示文档及获取调阅展示文档交易的请求。

交易的选择

表17　调阅展示角色交易表

角色	交易	选择
信息资源[EHR]调阅服务	获取专有信息	可选（O）
	获取展示文档	必须（R）
信息资源[EHR]使用者	获取专有信息	可选（O）
	获取展示文档	必须（R）

交易流程

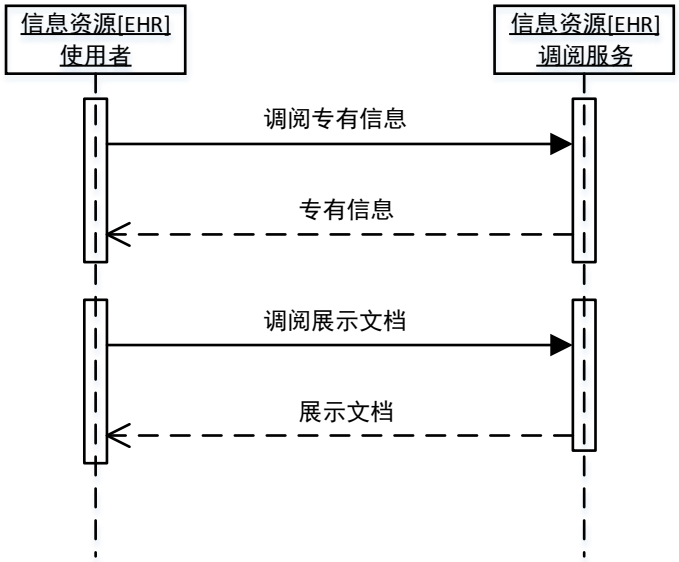

图33　调阅展示时序图

调阅专有信息交易由信息资源[EHR]使用者发起，信息资源[EHR]调阅服务角色向个人注册服务请求个人ID查询交易， 向信息资源[EHR]注册中心发起检索交易，返回索引信息给信息资源[EHR]使用者；信息资源[EHR]使用者可以根据索引信息向信息资源[EHR]调阅服务发起调阅展示文档交易，信息资源[EHR]调阅服务向文档源发起提取文档交易，并返回文档给信息资源[EHR]使用者展示。

6.2.3.4　信息资源[EHR]摘要调阅服务

信息资源[EHR]摘要调阅服务指提供特定信息资源[EHR]的摘要信息。

角色和交易

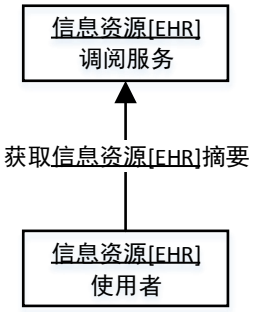

图34　EHR 摘要调阅角色交易图

- 信息资源[EHR]使用者发起获取信息资源[EHR]摘要信息的请求；
- 信息资源[EHR]调阅服务接收请求后反馈信息资源[EHR]摘要信息。

交易的选择

表18　信息资源[EHR]摘要调阅角色交易表

角色	交易	选择
信息资源[EHR]调阅服务	获取信息资源[EHR]摘要请求	必须（R）
信息资源[EHR]调阅消费者	反馈信息资源[EHR]摘要	必须（R）

交易流程

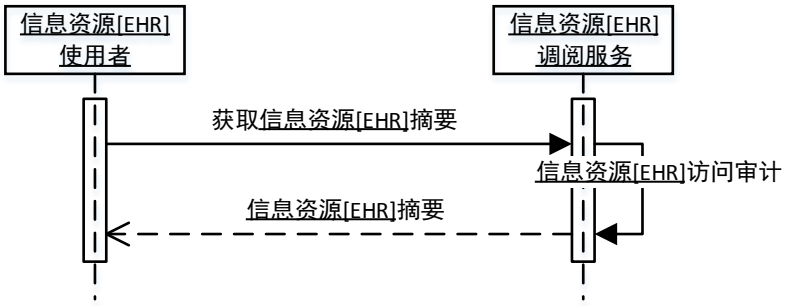

图35　EHR 摘要调阅用时序图

调阅信息资源[EHR]摘要交易由信息资源[EHR]使用者发起，信息资源[EHR]调阅服务角色向个人注册服务请求个人ID查询交易， 向信息资源[EHR]注册中心发起检索交易，返回索引信息给信息资源[EHR]使用者；信息资源[EHR]使用者可以根据索引信息向信息资源[EHR]调阅服务发起展示调阅摘要交易，信息资源[EHR]调阅服务向信息资源[EHR]发起提取摘要交易，并返回摘要文档给信息资源[EHR]使用者展示。

6.2.4　协同服务

6.2.4.1　服务概述

参见WS/T 448-2014平台功能和交易业务协同服务。

医疗卫生业务协同是指医疗卫生机构与机构之间通过省级人口健康综合管理平台实现业务的协同。通过医疗卫生业务协同，可以有效利用医疗资源，降低医疗成本，提高医疗质量。

角色和交易

医疗卫生业务协同服务包括三个角色：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方式把自己的功能和数据注册在医疗卫生业务协同服务组件中，医疗卫生业务协同服务组件可以对这些业务服务进行组装、编排并对外暴露出一组协同服务。协同服务使用者根据业务需要调用协同服务。医疗卫生业务协同服务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，并进行组装、编排后响应协同服务使用者的请求。

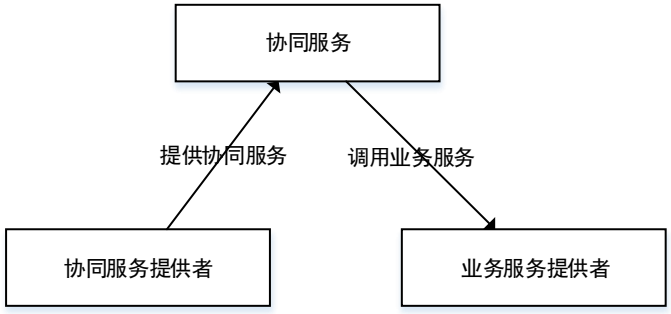

图36　区域医疗卫生协同服务角色交易图

角色的选择

表19　区域医疗卫生协同服务角色交易表

角色	交易	可选性
协同服务使用者	调用协同服务	必须（R）
业务服务提供者	调用业务服务	必须（R）
医疗卫生业务协同服务	调用协同服务	必须（R）
	调用业务服务	

交易流程

以双向转诊为例：

- 社区卫生服务中心作为协同服务使用者，调用医疗卫生业务协同服务组件中的双向转诊资源查询服务。
- 医疗卫生协同服务组件调用协议医院 A（作为业务服务提供者 A）的转诊资源查询服务。
- 协议医院 A（作为业务服务提供者 A）的转诊资源查询服务返回转诊资源响应给医疗卫生业务协同服务组件。
- 医疗卫生业务协同服务组件调用协议医院 B（作为业务服务提供者 B）的转诊资源查询服务。
- 协议医院 B（作为业务服务提供者 B）的转诊资源查询服务返回转诊资源响应给医疗卫生业务协同服务组件。
- 医疗卫生业务协同服务组件将收到的协议医院 A 的转诊资源响应和协议医院 B 的转诊资源响应整合后，作为协同服务的响应，返回给社区卫生服务中心。

6.2.4.2　实现选择

基于 ESB

ESB全称为Enterprise Service Bus，即企业服务总线。可以基于ESB提供的基于内容的路由和过滤来支撑医疗卫生业务协同。

基于 BPM

BPM 全称为 Business Process Manager，即业务流程管理。可以基于 BPM 的复杂的业务流程建模和流程引擎的能力来支撑医疗卫生业务协同。同时可以针对业务需求的变化，实现业务流程优化和业务流程重组。ESB 实现了业务服务的重用，BPM 实现了业务流程的重用。

基于事件（EDA）

EDA全称为Event-Driven Architecture，即事件驱动架构。它是一个异步地发布订阅模式。可基于EDA提供的发布订阅模式来支撑医疗卫生业务协同中异步形式的协同。

基于业务规则引擎（BRE）

业务规则引擎是一种嵌入在应用程序中的组件，实现了将业务决策从应用程序代码中分离出来，并使用预定义的语义模块编写业务决策。接受数据输入，解释业务规则，并根据规则做出业务决策。可基于BRE提供的业务规则来支撑医疗卫生业务协同。

6.3 资源存储服务

6.3.1 健康档案与电子病历数据服务

包括健康档案数据服务及电子病历数据服务。参见 WS/T 448-2014 平台功能和交易规范健康档案服务。

健康档案存储服务是以标准化的方式存储健康档案信息，为健康档案的共享和管理、基于健康档案的协同服务提供支持。健康档案存储服务基于XDS规范，包括文档库、文档注册、文档源和文档用户等几个角色。其中文档注册和文档库基于ebXML注册，SOAP，HTTP和SMTP等标准。

该服务同样适用于电子病历整合服务。

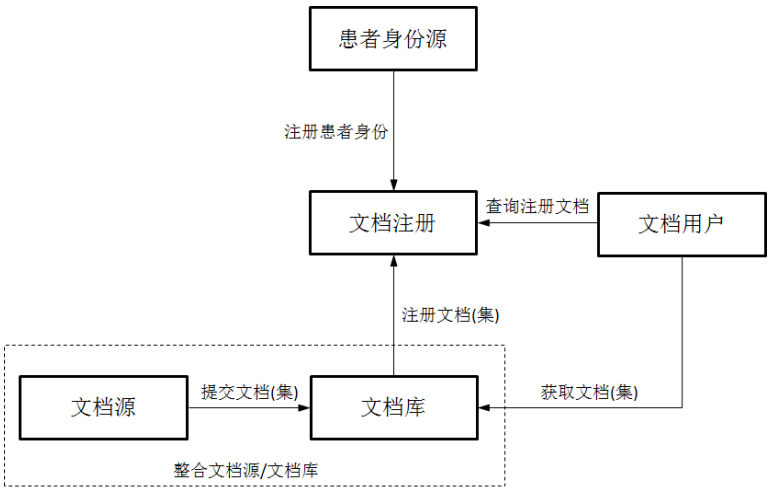

图37 健康档案存储服务角色交易图

6.3.1.1 角色与交易

表20 角色和交易关系表

角色	交易	选择
个人身份源	注册个人身份	可选(O)
文档注册	注册文档(集)	必须(R)
	查询注册信息	必须(R)
	获取文档(集)	可选(O)
文档库	提供文档(集)	必须(R)
	注册文档(集)	必须(R)
	获取文档(集)	必须(R)
文档用户	查询注册信息	必须(R)
	获取文档(集)	必须(R)
文档源	提供文档(集)	必须(R)
整合文档源/文档库	注册文档(集)	必须(R)

角色

包括以下角色：

——文档源：文档源是文档的发布者，它负责把文档发送给文档库。它提供给文档库足够的元数据资料，以满足文档库把文档信息注册到文档注册角色中。

——文档用户： 文档用户要求一个文档注册角色提供满足查询要求的文档信息,并且从文档库中获取一个或多个文档（集）。

——文档注册角色： 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。文档注册角色需要根据文档用户的特定查询条件返回文档（集）。文档注册时它会要求一些特定的卫生服务信息的隐私技术策略。

——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。它分配一个 URI 地址给文档注册角色供文档用户提取。

——个人身份源：个人身份源提供给每个个人一个唯一身份认证，并且维护个人的认证特征。个人身份源在进行文档交互过程中提供个人认证的有效性给文档注册角色。

——整合文档源/文档库： 整合文档源/文档库结合了文档源和文档库的功能，直接对外提供文档注册信息和获取文档服务。

交易

以健康档案为代表的资源存储服务包括以下交易：

——提交文档（集）：文档源角色发起提供和注册文档集交易。对提交的集合中的每一个文档，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。

——注册文档（集）：文档库角色发起注册文档集交易。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，文档注册角色要确保文档元数据是正确的。如果一个或多个文档元数据校验失败，此注册文档集交易就全部失败。为支持复合文档，一个 XDS 文档可能是一个多部分文档。文档库必须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。

——查询注册信息：查询注册信息交易由文档用户角色向文档注册角色发起。文档注册角色按照文档用户角色指定的查询条件搜索本地文档注册,将返回一个包含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，其中还有每个相应文档的位置和标识符。

——获取文档（集）：文档用户角色发起获取文档交易。文档库将返回文档用户指定的文档。为支持复合文档，XDS 文档可以是一个多部分文档。文档用户必须采取适当的措施使得用户能够获取多部分文档的内容。

——注册个人信息：注册个人信息交易用来传送个人标识。它传递个人标识和相关的人口学数据，这些标识符和人口学数据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 集成模式中目的是把已经在相关域中注册的个人标识符传递到注册者。

6.3.1.2 文档处理

表21 文档处理角色交易关系图

角色	交易	选择
文档源	文档替换	必须（R）
	文档新增	必须（R）
	文档改变	必须（R）
	文件夹管理	必须（R）
整合文档源/文档库	文档替换	必须（R）
	文档新增	必须（R）
	文档改变	必须（R）
	文件夹管理	必须（R）

文档替换

文档源和整合文档源/文档库应当提供这样的功能，提交一份文档替换已存在在文档库中的另一个文档。分组文档用户可以提交用于取代的最新元数据和ID。

文档新增

文档源和集成文档源/存储库应当提供这样的功能，提交一份文档用于增补已存在在文档库中的另一个文档。

文档转换

文档源和集成文档源/存储库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。

6.3.1.3 文件夹管理

文档源应该提供以下操作：

- 创建一个文件夹
- 添加一个或多个文档到一个文件夹中

6.3.2 全员人口数据服务

6.3.2.1 基本人口信息存储服务

提供基本人口信息的存储与获取，支持将多个域来源的同一个人的信息进行合并存储。

角色和交易

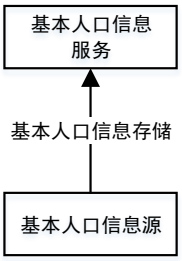

图38 基本人口信息存储服务角色交易图

基本人口信息存储服务涉及两个角色，基本人口信息源和基本人口信息存储服务组件。基本人口信息源向基本人口信息存储服务组件提交基本人口信息。

角色交易选择

表22　个人身份注册角色-交易关系表

角色	交易	选择
基本人口信息源	提交基本人口信息	必须（R）
基本人口信息存储服务	人口信息匹配处理	必须（R）
	基本人口信息存储	必须（R）

交易流程

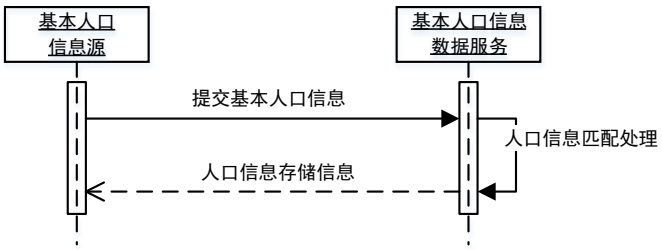

图39　基本人口信息提交存储时序图

- 基本人口信息源向基本人口信息存储服务提交基本人口信息；
- 基本人口信息存储服务进行人口信息匹配处理，并进行人口信息的存储返回人口信息存储信息。

交易消息

基本人口信息、人口信息存储信息。

6.3.2.2　基本人口信息查询服务

提供基本人口信息的查询。

角色和交易

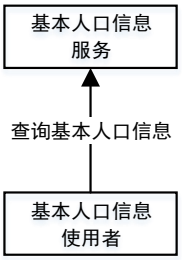

图40　基本人口信息查询服务角色交易图

基本人口信息查询服务涉及两个角色，基本人口信息使用者和基本人口信息存储服务组件。基本人口信息使用者向基本人口信息存储服务组件查询基本人口信息。

角色交易选择

表23　个人身份注册角色-交易关系表

角色	交易	选择
基本人口信息使用者	查询基本人口信息	必须（R）
基本人口信息存储服务	查询基本人口信息	必须（R）

交易流程

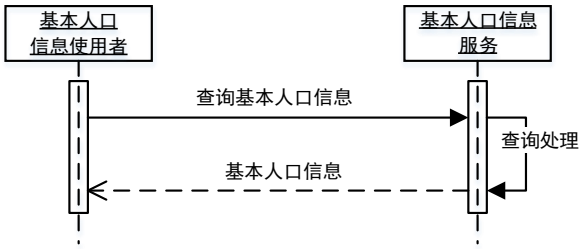

图41　基本人口信息提交存储时序图

- 基本人口信息使用者向基本人口信息存储服务查询基本人口信息；
- 基本人口信息存储服务进行人口信息查询处理，返回基本人口信息。

交易消息

基本人口信息。

6.3.2.3　流动人口数据存储服务

提供流动人口信息的存储与获取，支持将多个域来源的同一个人的信息进行合并存储。

角色和交易

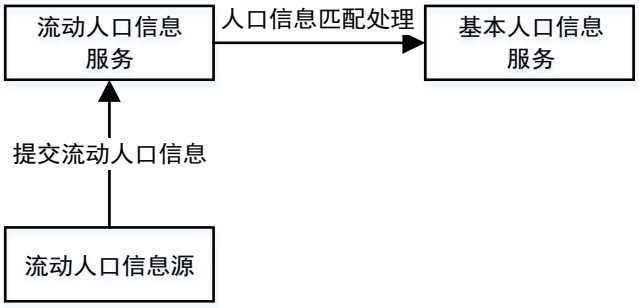

图42　流动人口信息存储服务角色交易图

流动人口信息存储服务涉及三个角色，流动人口信息源、流动人口数据服务组件、基本人口数据服务组件。基本人口信息源向基本人口信息存储服务组件提交基本人口信息，基本人口信息服务提供人口信息匹配处理。

角色交易选择

表24　个人身份注册角色-交易关系表

角色	交易	选择
流动人口信息源	提交基本人口信息	必须（R）
流动人口信息服务	人口信息匹配处理	必须（R）
	流动人口信息存储	必须（R）
基本人口信息服务	人口信息匹配处理	必须（R）

交易流程

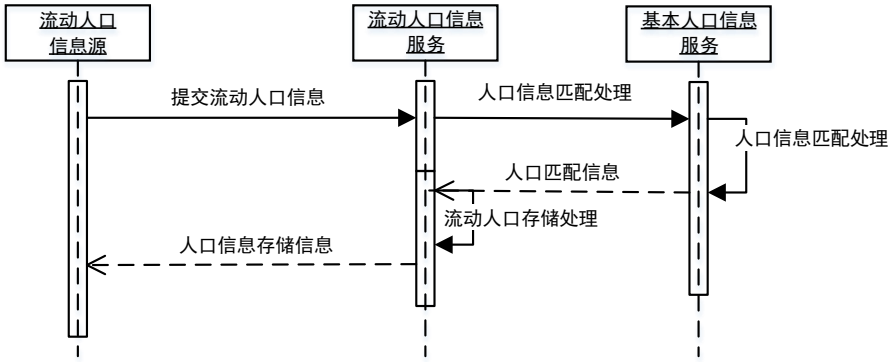

图43　流动人口信息提交存储时序图

- 流动人口信息源向流动人口信息服务提交流动人口信息；
- 流动人口信息服务向基本人口信息服务请求人口匹配处理；
- 流动人口信息服务进行流动人口存储处理处理，并将流动人口信息的存储结果返回流动人口信息源。

交易消息

基本人口信息、人口信息存储信息。

6.3.2.4　流动人口信息查询服务

提供流动人口信息的查询。

角色和交易

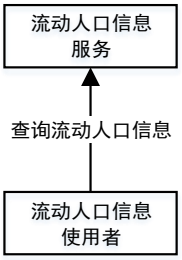

图44　基本人口信息查询服务角色交易图

基本人口信息查询服务涉及两个角色，基本人口信息使用者和基本人口信息存储服务组件。基本人口信息使用者向基本人口信息存储服务组件查询基本人口信息。

角色交易选择

表25　个人身份注册角色-交易关系表

角色	交易	选择
基本人口信息使用者	查询基本人口信息	必须（R）
基本人口信息存储服务	查询基本人口信息	必须（R）

交易流程

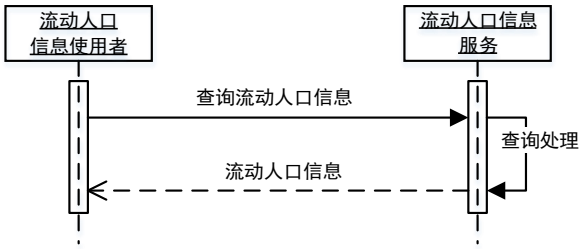

图45　基本人口信息提交存储时序图

- 流动人口信息使用者向流动人口信息服务查询基本人口信息；
- 流动人口信息存储服务进行人口信息查询处理，返回流动人口信息。

交易消息

流动人口信息、基本人口信息。

6.3.2.5　计划生育人口数据存储服务

提供计划生育人口信息的存储与获取，支持将多个域来源的同一个人的信息进行合并存储。

角色和交易

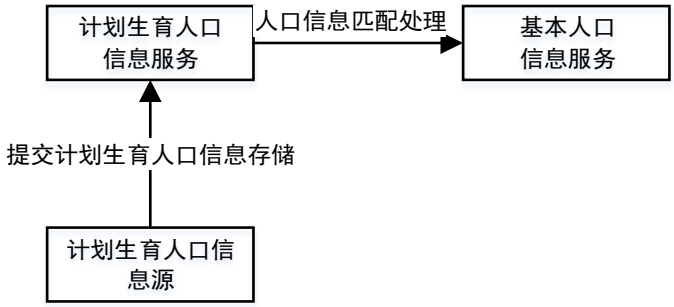

图46　基本人口信息存储服务角色交易图

计划生育人口信息存储服务涉及三个角色，计划生育人口信息源、计划生育人口信息服务组件、基本人口服务组件。

角色交易选择

表26　个人身份注册角色-交易关系表

角色	交易	选择
计划生育人口信息源	提交计划生育人口信息	必须（R）
计划生育人口信息服务	提交计划生育人口信息(实现)	必须（R）
	计划生育人口信息存储处理	必须（R）
基本人口信息服务	人口信息匹配处理	必须（R）

交易流程

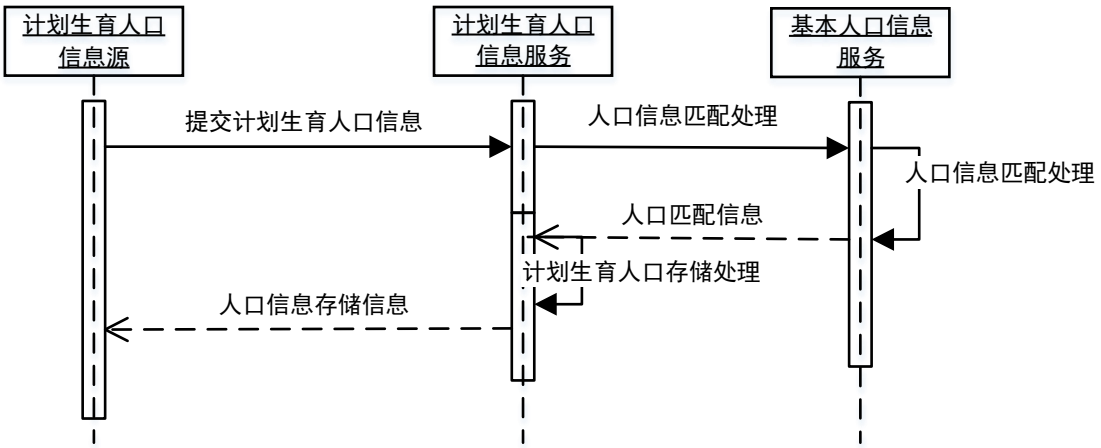

图47　基本人口信息提交存储时序图

- 计划生育人口信息源向计划生育人口信息服务提交计划生育人口信息；
- 计划生育人口信息服务向计划生育人口信息服务请求人口匹配处理；
- 计划生育人口信息服务进行计划生育人口存储处理处理，并将计划生育人口信息的存储结果返回计划生育人口信息源。

交易消息

计划生育人口信息、人口信息存储信息。

6.3.2.6　计划生育人口信息查询服务

提供计划生育人口信息的查询。

角色和交易

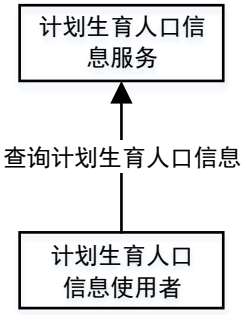

图48　基本人口信息查询服务角色交易图

计划生育人口信息查询服务涉及两个角色，计划生育人口信息使用者和计划生育人口信息存储服务组件。计划生育人口信息使用者向计划生育人口信息存储服务组件查询计划生育人口信息。

角色交易选择

表27　个人身份注册角色-交易关系表

角色	交易	选择
计划生育人口信息使用者	查询计划生育人口信息	必须（R）
计划生育人口信息存储服务	查询计划生育人口信息	必须（R）

交易流程

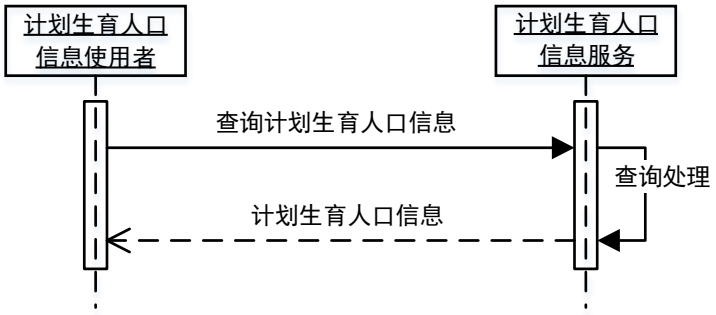

图49　计划生育人口信息提交存储时序图

- 计划生育人口信息使用者向计划生育人口信息存储服务查询计划生育人口信息；
- 计划生育人口信息存储服务进行人口信息查询处理，返回计划生育人口信息。

交易消息

计划生育人口信息。

6.4　人口健康综合管理服务

综合卫生管理服务通过对健康影响因素、健康状况、疾病控制与疾病管理、妇幼保健、卫生监督、医疗服务、药品供应保障、卫生资源等指标的获取、健康档案的数据抽取、分析、数据挖掘，实现对业务服务的监管与业务指导。

6.4.1 卫生关键指标服务

角色和交易

卫生关键指标服务包括三个角色：卫生关键指标服务组件、综合卫生管理者和综合卫生管理对象。综合卫生管理者通过卫生关键指标服务，向综合卫生管理对象提供卫生关键指标服务。卫生关键指标服务根据综合卫生管理者的服务请求，通过调用卫生统计指标服务，向综合卫生管理对象提供相应的关键指标服务。

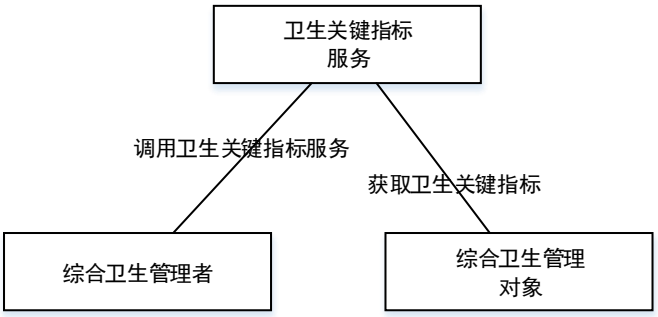

图50 卫生关键指标服务角色交易图

角色的选择

表28 卫生关键指标服务角色交易表

角色	交易	可选性
综合卫生管理者	调用卫生关键指标服务	必须（R）
	获取卫生关键指标	
	卫生关键指标通知	
综合卫生管理对象	调用卫生关键指标服务	必须（R）
	获取卫生关键指标通知	
	获取卫生关键指标	
卫生关键指标服务	提供卫生关键指标服务	必须（R）
	指供卫生关键指标通知	

交易流程

综合卫生管理服务交易流程如下：

- 卫生行政管理机构、卫生业务机构管理人员作为综合卫生管理者，调用综合卫生管理服务组件中相应的管理服务，获取卫生关键指标。
- 综合卫生管理服务组件提供相应的管理服务,这些服务包括疾病控制与疾病业务服务监管、妇幼保健服务监管、卫生监督业务监管、医疗服务业务监管、药品供应保障业务服务监管、卫生资源管理，以及健康影响因素、健康状况分析等关键指标。
- 综合卫生管理服务组件向综合卫生管理对象发送卫生统计指标通知；

- 各业务服务机构作为综合卫生管理对象获取卫生关键指标结果。个人或机构管理者亦可获取相应机构的卫生关键指标结果信息。

6.4.2 资源综合查询服务

角色和交易

综合健康查询服务包括三个角色：综合健康查询服务组件、综合健康信息提供者和综合健康服务使用者。综合健康使用者通过综合健康查询服务查询综合健康信息。综合健康查询服务向综合健康信息提供者获取相应的综合健康信息，并依据综合健康查询服务使用者的请求，向其提供综合健康信息。

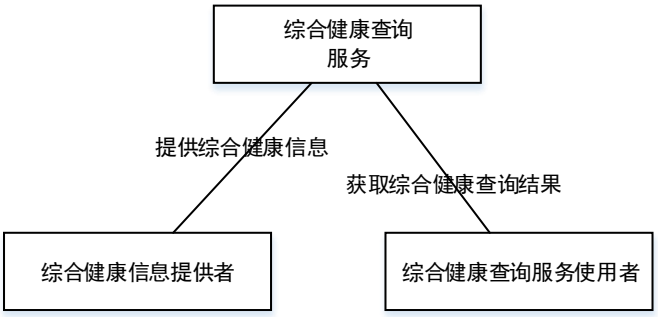

图51 综合健康查询服务角色交易图

角色的选择

表29 区域医疗卫生协同服务角色交易表

角色	交易	可选性
综合健康查询服务使用者	获取综合健康查询结果信息	必须（R）
综合健康信息提供者	提供综合健康信息	
综合健康查询服务	获取综合健康信息	必须（R）
	提供综合健康查询结果	

交易流程

综合健康查询服务交易流程如下：

- 卫生行政管理机构、卫生业务机构管理人员以及综合卫生管理对象作为综合健康查询服务的使用者，调用综合健康查询服务；
- 综合健康查询服务组件通过综合健康信息提供者获取综合健康信息；
- 综合健康查询服务组件向综合健康查询服务使用者提供查询结果信息。

6.4.3 综合数据分析服务

角色和交易

综合数据分析服务通过一定的数学模型，对综合卫生数据进行综合分析，提供预后、优化参数等决策支持。综合数据分析服务包括三个角色：综合卫生分析服务使用者、综合数据分析服务组件、综合卫生数据分析数学模型提供者。综合分析数学模型提供者依据分析的要求建立数学计算模型(分析规则)；数据分析服务组件依据数学模型对获取的数据进行数据分析；分析结果存储在知识库中；综合分析服务使用者通过综合分析服务查询分析结果，综合分析服务提供综合数据分析结果。

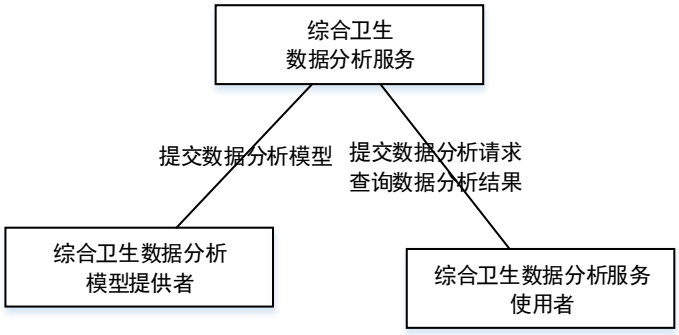

图52　区域医疗卫生协同服务角色交易图

角色的选择

表30　区域医疗卫生协同服务角色交易表

角色	交易	可选性
综合卫生数据分析使用者	提交综合卫生数据分析服务请求	
	查询综合卫生数据分析结果	必须（R）
综合卫生数据分析模型提供者	提交综合卫生数据分析模型	必须（R）
综合卫生管理服务	获取综合卫生数据分析请求	必须（R）
	获取综合卫生数据分析模型	
	提供数据分析结果	必须（R）

交易流程

综合卫生管理服务交易流程如下：

- 卫生行政管理机构、卫生业务机构管理人员作为综合卫生管理者，调用综合卫生管理服务组件中相应的管理服务。
- 综合卫生管理服务组件提供相应的管理服务,这些服务包括疾病控制与疾病业务服务监管、妇幼保健服务监管、卫生监督业务监管、医疗服务业务监管、药品供应保障业务服务监管、卫生资源管理，以及健康影响因素、健康状况分析等。
- 各业务服务机构作为综合卫生管理对象可通过直接获取、订阅等方式获取综合管理结果。个人或机构管理者亦可获取相应机构的综合卫生管理服务结果信息。

6.5　信息安全与隐私服务

6.5.1　用户管理和权限控制

实体认证

a) 应确保访问省级人口健康综合管理平台的所有实体（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：
   - 对省级人口健康综合管理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；
   - 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/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 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。

c) 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。

d) 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。

实体授权

a) 应根据用户对省级人口健康综合管理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。

b) 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；
- 提供增加、修改、删除和查询用户权限的功能；
- 能够创建、修改数据访问规则，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）；
- 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。

实体访问控制

应启用访问控制功能，依据安全策略控制用户对平台系统的访问，满足以下功能要求：

a) 标识和鉴别系统用户的过程
- 应符合功能 6.7.1.1（实体认证）

b) 角色的职能分割
- 应符合功能 6.7.1.2（实体授权）

c) 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。

6.5.2 信息安全

病人访问管理

a) 允许并管理病人通过平台访问个人的健康信息，病人在进行系统访问时进行有效的身份认证
   - 应符合功能 6.7.1.1（实体认证）
b) 为一个医疗服务机构来管理病人对医疗信息的访问
   - 应符合功能 6.7.1.2（实体授权）
   - 应符合功能 6.7.1.3（实体访问控制）

不可抵赖

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。

数据安全传递

a) 应对数据交换的参与者双方进行有效的身份认证：
   - 应符合功能 6.7.1.1（实体认证）
b) 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
c) 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

d) 应保障交换数据的真实性及不可抵赖性：
- 应符合功能 6.7.2.2（不可抵赖）

数据安全路由

a) 在通信双方建立连接之前，应用系统应进行会话初始化验证：
- 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

b) 应确保只和认证及授权过的来源和目的地进行健康档案的数据传递：
- 应符合功能 6.7.1.1（实体认证）
- 应符合功能 6.7.1.2（实体授权）
- 应符合功能 6.7.1.3（实体访问控制）

c) 应保障传递数据的安全性：
- 应符合功能 6.7.2.3（数据安全传递）

信息验证

a) 应确保健康记录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

b) 应提供健康档案的编写者进行增加和修改健康档案的内容；

c) 应提供健康档案的编写者进行健康档案的验证功能：
- 宜采用数字签名/验签技术实现
- 应标明健康档案是否被验证
- 验证过程记录的文件要有保留

d) 能够为通过认证和授权的用户情况提供健康档案的验证：
- 应符合功能 6.7.1.1（实体认证）
- 应符合功能 6.7.1.2（实体授权）
- 应符合功能 6.7.1.3（实体访问控制）

6.5.3 隐私保护

a) 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：
- 应符合功能 6.7.1.1（实体认证）；
- 应符合功能 6.7.1.2（实体授权）；
- 应符合功能 6.7.1.3（实体访问控制）；
- 应符合功能 6.7.2.2（不可抵赖性）；
- 应符合功能 6.7.2.3（数据安全传递）；
- 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电子健康记录（如药物，条件，敏感的文件）的隐藏功能。

b) 应提供匿名化服务：
- 保护患者的隐私和安全,确保在信息平台中以及提供正常医疗服务以外的(例如医疗保险、管理以及某种形式的研究）传递中使用的患者资料不向非授权用户透露患者的身份；

c) 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。允许信息平台用户管理患者/居民的特定许可指示，例如根据法律法规的需要和允许，阻止和屏蔽某一医疗服务提供者访问健康档案或者在紧急治疗情况下不经许可直接开放健康档案。

6.5.4 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。

7 数据采集规范

7.1 数据采集范围

7.1.1 人口健康数据

规范待定。

7.1.2 医疗业务数据

医疗业务数据采集范围参考卫生部《电子病历基本架构与数据标准（试行）》的规定的7个业务域16类62个活动产生的活动记录。具体数据标准需符合《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》、《WS 365-2011城乡居民健康档案基本数据集》，文档格式按照《WS XXX-2012 电子病历共享文档规范》。

7.1.3 健康档案数据

健康档案数据采集范围参考卫生行业标准《WS 365-2011城乡居民健康档案基本数据集》的规定。具体数据标准需符合《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》，文档格式按照《WS XXX-2012 健康档案共享文档规范》。

7.1.4 药品供应保障业务数据

规范待定。

7.1.5 医疗保障（新农合）业务数据

规范待定。

7.1.6 卫生关键指标

卫生行业标准所规定的卫生统计指标是基本的卫生指标，也是关键的卫生统计指标，本规范所指卫生关键指标主要包括以下卫生统计指标：

——WS/T XXXXX 2-XXXX 卫生统计指标第 2 部分居民健康状况；
——WS/T XXXXX.3-XXXX 卫生统计指标第 3 部分健康影响因素；
——WS/T XXXXX.4-XXXX 卫生统计指标第 4 部分疾病控制；
——WS/T XXXXX.5-XXXX 卫生统计指标第 5 部分妇幼保健；
——WS/T XXXXX.6-XXXX 卫生统计指标第 6 部分卫生监督；
——WS/T XXXXX.7-XXXX 卫生统计指标第 7 部分医疗服务；
——WS/T XXXXX.8-XXXX 卫生统计指标第 8 部分药品与材料供应保障；
——WS/T XXXXX.9-XXXX 卫生统计指标第 9 部分医疗保障新型农村合作医疗；
——WS/T XXXXX.10-XXXX 卫生统计指标第 10 部分卫生资源。

7.2 数据采集机制

7.2.1 医疗数据采集机制

医疗数据的采集主要从市县级区域卫生信息平台以及省属医院获取。分为下级区域卫生信息平台或医院信息平台主动推送和省级人口健康综合管理平台主动提取两种方式。应根据项目实施环境的具体情况在方案中选择。

在省属医院中，对于门急诊业务，在患者接受了诊疗业务服务后，由医院卫生信息平台将相关数据按照标准规范整理汇集后提交省级人口健康综合管理平台。对于住院业务，患者办理登记入院，接受了各种治疗，当办理出院结算或者办理了离院手续时，医院信息系统须汇总全部已产生的诊疗数据填报提交。

7.2.2 健康档案数据采集机制

健康档案数据的采集主要从市级区域卫生信息平台获取。分为下级区域卫生信息平台主动推送和省级人口健康综合管理平台主动提取两种方式。应根据项目实施环境的具体情况在方案中选择。

7.2.3 卫生关键指标采集机制

按照国家卫生统计指标相关规定，卫生统计指标调查方法采用抽样调查、普查、全面调查以及专项调查方式分别对不同的指标进行采集。采集范围依据采集指标的不同目的与方法，主要包括全国范围、预定的监测点、医疗机构、特定人群、特定区域等；采集频率依据不同指标有实时、不定期、每月、每季度、半年、1年、5年、10年不等；采集方式包括从相关的信息系统适时查询或由专门的直报系统按时填报。

对于基于健康档案的区域卫生信息平台，如健康档案采集范围已经实现全覆盖，应采用通过健康档案提取的方式采集相关指标信息。

8 IT 基础设施规范

8.1 基本要求

用于搭建省级人口健康综合管理平台的IT基础设施（包括基础软件、数据库、服务器、存储、网络等），应满足以下基本技术要求：

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 应用服务器软件

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) 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) 可靠性要求
   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）软件

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 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) 应采用技术来保证平台 7*24 小时的运行；
   2) 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。
d) 功能要求

1) 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；
2) 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；
3) 支持标准 XML 数据的格式转换，可以通过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) 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

用于搭建省级人口健康综合管理平台的数据库，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) 支持主流的备份软件和数据同步软件；
4) 兼容主流的应用服务器架构；
5) 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
- 数据库集群或分布式数据库

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

省级人口健康综合管理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：

a) 配置合理：服务器的资源配置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) 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；
d) 高能效：服务器自身应该具有较高的性能/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《HJ 2507-2011 环境标志产品技术要求 网络服务器》的要求。

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
1) 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。
2) 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。

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

省级人口健康综合管理平台选择主机系统应具备多种高可靠性保护措施，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，宜包含但不限于：RAID0、1、0+1、5 等级别
2) RAID 卡宜支持缓存电池保护

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 和网络接口应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省级人口健康综合管理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

存储系统应满足省级人口健康综合管理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稳定性、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：

a) 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。
b) 可扩展性：存储网络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。
c) 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。
d) 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。
e) 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，抵御病毒攻击、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构模型和技术。
f) 标准开放性：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 存储可用性要求

存储系统需提供全年不断电无停止服务，确保高可靠性：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%；
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) 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；
g) 产品电位接地，防止触电事故；
h) 尺寸、规格、形状合理，以免倾斜倒伏，碰撞；
i) 产品材质耐温，散热；

j） 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，应实现 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

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，本规范定义了基本、中级、高级三个级别的存储配置要求。各地市宜根据结合实际情况，参考以下配置要求。

基本级别存储配置要求

平台在线存储系统容量估算：采取集中式存储系统，注册系统、索引系统、HER 交易缓存（HIAL）和 HER 数据系统约为 80-100GB/年。影像数据的存储配置应单独计算。

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；
- 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。
- 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。
- 应 SAS/SATA 硬盘，可支持 SSD/FC/硬盘。支持 300/450/600GB 高转速 SAS 磁盘，支持 500/1000/2000GB 高转速 SATA II 磁盘，实配容量≥1TB；最大扩展容量≥80TB。
- 大缓存，缓存≥8GB，最大缓存≥24GB;

b） 灾备系统要求：
- 支持本地的连续数据保护功能，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。
- 可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。
- 应支持远程容灾功能，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 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≥2TB，最多支持存储容量≥200TB
- 支持 LT03\LT04\LT05 驱动器

中级级别存储配置要求

平台在线存储系统容量估算：采取集中式存储系统，注册系统、索引系统、EHR交易缓存（HIAL）和EHR数据系统约为200-500GB/年。影像数据的存储配置应单独计算。

存储配置要求：

d) 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 SATA II 磁盘，支持 100GB SSD 硬盘，实配容量≥3TB；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≥16GB，最大缓存≥32GB；
- 异构整合、集中部署，统一管理，降低整体拥有成本（TCO）。

e) 灾备系统要求：

- 支持本地的连续数据保护功能，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。

f) 离线存储要求：

- 可选用虚拟带库或物理带库设备，支持 LT03\LT04\LT05 驱动器
- 支持 FC 或 IP 主机接口
- 配置容量≥6TB，最多支持存储容量≥200TB
- 支持 LT03\LT04\LT05 驱动器

高级级别存储配置要求

在线存储系统容量估算：采取集中式存储系统，注册系统、索引系统、EHR交易缓存（HIAL）和EHR数据系统约为600GB-1TB/年。各地市可结合实际情况增配存储容量。影像数据的存储配置应单独计算。

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；
- 宜全面支持 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 SATA II 磁盘，宜支持

100GB SSD 硬盘，实配容量宜≥6TB；最大扩展容量宜≥200TB，灵活配置满足不同层级数据存储需求；

- 高缓存，缓存宜≥32GB，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）。

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 LT03\LT04\LT05 驱动器
- 支持 FC 或 IP 主机接口
- 配置容量宜≥12TB，最多支持存储容量宜≥400TB
- 支持 LT03\LT04\LT05 驱动器

8.6 网络系统

8.6.1 省级人口健康综合管理平台网络参考架构

本技术规范中的平台网络参考架构在《基于健康档案的区域卫生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，如下图所示：

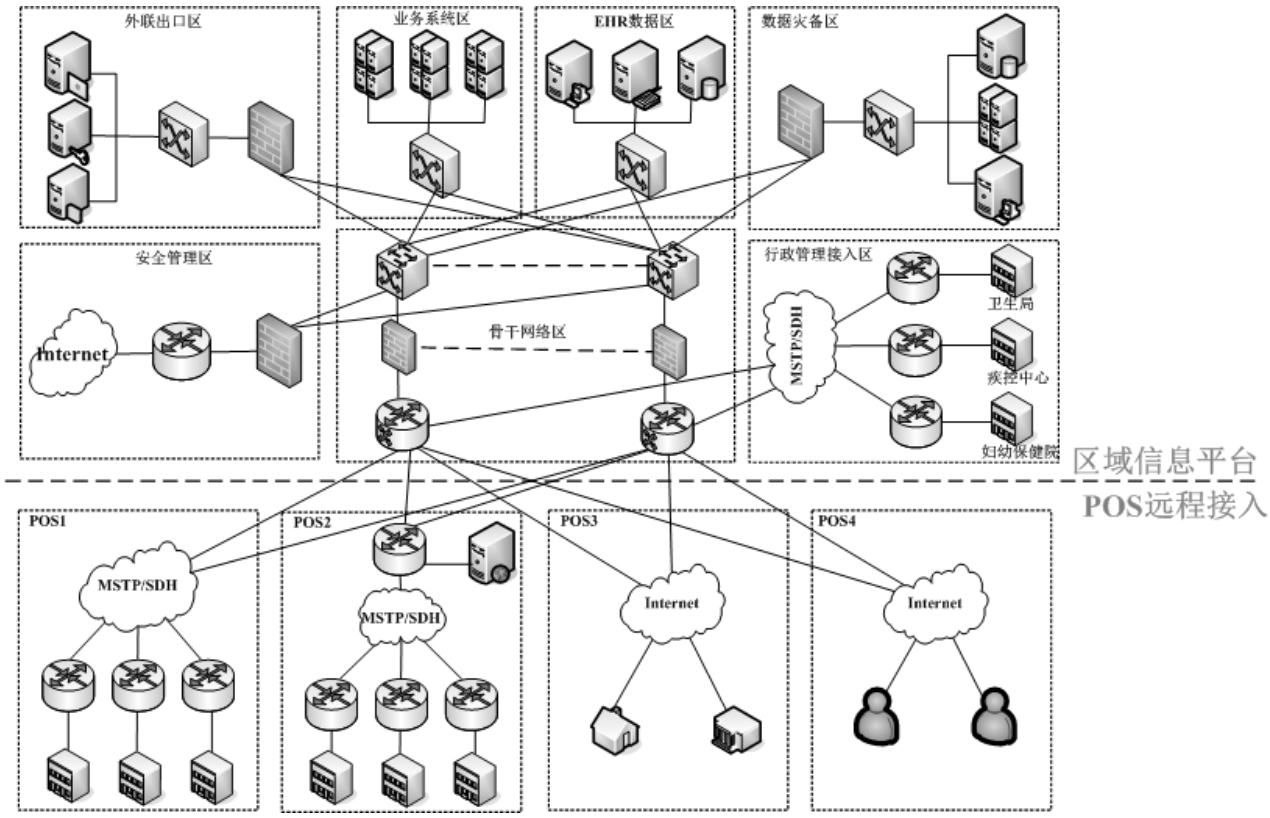

图53　省级人口健康综合管理平台整体网络架构图

整体网络应由两大部分组成：省级人口健康综合管理平台网络和POS远程接入。

a) 省级人口健康综合管理平台网络主要负责支撑省级人口健康综合管理平台的运行和管理，以及与外部系统的连接。

b) POS 远程接入主要负责各 POS 点的接入，实现数据交换和服务调用。

8.6.2 省级人口健康综合管理平台区域划分

省级人口健康综合管理平台网络按照功能从逻辑上划分，应至少包括以下区域， 各区域间需通过防火墙进行安全隔离。服务点系统（POS）分类描述参见附录

a) 骨干网络区域

该区域主要实现以下功能

1) 对各 POS 远程接入链路进行汇聚
2) 连接卫生区域信息平台各区域
3) 对卫生区域信息平台各区域数据进行高速转发处理

b) 业务系统区域

该区域主要包括以下业务相关设备

1) 应用服务器
2) 数据库服务器
3) 中间件服务器
4) 数据存储设备

c) 安全管理区域

该区域主要实现以下功能

1) 证书服务器
2) 身份认证
3) 漏洞扫描
4) 入侵检测
5) 网络管理

d) 数据灾备区域

该区域主要实现以下功能

1) 作为远程灾备
2) 实现业务系统与灾备区域数据的同步
3) 通过高速链路直接与核心交换机

e) 外联出口区

该区域主要实现以下功能

1) 负责连接外联单位
2) 将来实现域间互连互通时提供开放接口

f) 管理接入区

该区域主机负责将省级人口健康综合管理平台的行政管理部门接入数据中心

g) 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/Adaptor），将POS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

h） POS-2 接入

POS-2接入要求：POS内业务系统通过文档重构的引擎/适配器（Engine/Adaptor），将数据转换成标准的业务文档格式，提交到信息平台

i） 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/Adaptor），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

j） 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

8.6.3 网络带宽要求

接入带宽要求

a） 三级医院接入带宽宜≥1000M
b） 二级医院接入带宽宜≥100M
c） 社区服务中心接入带宽宜≥8M
d） 社区服务站接入带宽宜≥4M
e） 行政管理接入带宽宜≥100M
f） 其他医疗卫生机构应结合业务要求进行配置

省级人口健康综合管理平台骨干区域带宽要求

a） 对于 100 万人口以下规模的区域，核心交换设备宜达到千兆接入速率；
b） 对于 100 万人口以上规模的区域，核心交换设备宜达到万兆接入速率。

8.6.4 骨干网络设计要求

网络可靠性

a） 设备级别可靠性要求
- 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

b） 网络级别可靠性要求
- 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 以及组播路由快速收敛
- 核心设备应支持虚拟路由冗余协议（VRRP，Virtual Router Redundancy Protocol）
- 核心设备应支持快速环网保护协议（RRPP，Rapid Ring Protection Protocol）
- 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

8.6.5 服务点系统接入设计要求

网络可靠性

a) 支持双出口备份，选择两家不同的运营商提供的物理链路接入作为互备
b) 支持接入设备双机备份
c) 支持快速切换
   1) 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 1～2 秒内发现故障
   - VRRP 在 3～4 秒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
   2) 网关链路异常时，需要 VPN 隧道能快速切换

8.6.6 网络规划要求

IP 地址规划

a) 省级人口健康综合管理平台 IP 地址规划要求
   - IP 地址的分配必须采用 VLSM(Variable Length 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
b) 在规划 IP 地址时，应结合本地电子政务外网或其他资源网络（如新农合网，社保网）的部署，综合考虑 IP 地址资源分配。
c) IP 地址规划需参照的标准和规范
   - RFC 1366 《Guidelines For Management of IP Address Space》
   - RFC 1466 《Guidelines For Management of IP Address Space》
   - RFC 1597 《Address Allocation for Private Internets》
   - RFC 1918 《Address Allocation for Private Internets》
   - RFC 0793 《Transmission Control Protocol》
   - RFC 0791 《Internet Protocol》

8.6.7 网络管理要求

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。

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。

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。

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

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

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

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

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。

备件管理

a) 基础数据管理：
   - 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
b) 备件管理
   - 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

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。

表31 RTO/RPO 与灾难恢复能力等级的关系

灾难恢复能力等级	RTO	RPO
1	2 天以上	1 天至 7 天
2	24 小时以后	1 天至 7 天
3	12 小时以上	数小时至 1 天
4	数小时至 2 天	数小时至 1 天
5	数分钟至 2 小时	0 至 30 分钟
6	数分钟	0

省级人口健康综合管理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级及以上灾备等级。

对于基本规模省级人口健康综合管理平台，灾难备份系统的建设目标是RPO为数小时至1天，RTO为数小时至2天。

对于中级规模省级人口健康综合管理平台，灾难备份系统的建设目标是RPO≤30分钟，RTO为数分钟至2小时。

对于高级规模省级人口健康综合管理平台，灾难备份系统的建设目标是RPO，灾难备份系统的建设目标，灾难发生后数据不容丢失，即RPO=0，RTO为数分钟。

8.8 可管理性要求

8.8.1 基本要求

省级人口健康综合管理平台提供的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；省级人口健康综合管理平台做为服务平台，也应满足可管理型的要求。

8.8.2 服务级别协议

省级人口健康综合管理平台的服务提供者将为区域内相关医疗卫生机构以及行政管理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 需要规范的内容如下（包括且不限于）

- 分配给客户的最小带宽；
- 客户带宽极限；
- 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。

8.8.3 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，具有要求如下：

- 用户可以通过交互接口来请求服务。平台的所有服务目录存放在服务目录里，用户可以通过门户方式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，或者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程，记录，审批并实施服务的变更。

8.8.4 配置/部署管理

- 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。最大程度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。平台应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对业务高峰。
- 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。

8.8.5 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。在虚拟化的环境中，监控任务更为困难，也更为关键。系统能够 ：

- 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

8.8.6 容量规划

省级人口健康综合管理平台内的系统、软件和数据容量将不断增长。应该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。

8.8.7 事件管理

平台服务的提供者，应提供相应的事件管理功能，记录事件发生事件，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

8.8.8 资产管理

应提供IT基础设施资产管理功能，满足资产审计，折旧，变更，淘汰等管理要求。

8.9 机房建设

省级人口健康综合管理平台机房建设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。

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) 应从安全技术、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

物理安全主要是指省级人口健康综合管理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

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。

安全区域边界安全

a) 在省级人口健康综合管理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。

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。

9.3.3 服务端系统安全

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

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。

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：

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。

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

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。

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或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

a) 用户管理和权限控制
   - 应符合功能 6.7.1（用户管理和权限控制）
b) 信息安全
   - 应符合功能 6.7.2（信息安全）
c) 隐私保护
   - 应符合功能 6.7.3（隐私保护）
d) 审计追踪
   - 应符合功能 6.7.4（审计追踪）
e) 剩余信息保护
   - 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。
f) 软件容错
   - 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；
   - 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
   - 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、电子健康档案和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） 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：

- 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 机构接入规范要求

10.1 机构接入规范内容

机构接入规范应包括以下部分：

- 功能服务接入规范，机构应实现注册服务、健康档案整合服务、健康档案管理服务、健康档案调阅服务、健康档案协同服务、健康档案浏览器、安全与隐私服务接口。
- 信息服务接入规范，根据机构类型的不同，机构应实现个人基本信息、主要疾病和健康问题摘要信息、儿童保健信息、妇女保健信息、疾病控制信息、疾病管理信息、医疗服务信息的服务接口。
- 机构数据采集接口规范，应遵循《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 365-2011 城乡居民健康档案基本数据集》，文档格式按照《WS XXX-2012 卫生信息共享文档规范》的规范要求，例如医疗机构数据采集接口规范、基层医疗卫生机构数据采集接口规范、公共卫生机构数据采集接口规范。

10.2 功能服务接入规范

10.2.1 注册服务调用

POS系统在进行居民/患者、医疗卫生人员、医疗卫生机构、医疗卫生术语登记时，应调用省级人口健康综合管理平台的注册服务，省级人口健康综合管理平台对这些实体提供唯一的标识，以实现居民健康档案共享和区域业务协同。

10.2.2 健康档案整合服务调用

POS系统通过调用省级人口健康综合管理平台的健康档案整合服务，实现需上传到区域的相关数据的抽取、转换与加载，或者按省级人口健康综合管理平台的规范要求开放相关接口给省级人口健康综合管理平台调用。

10.2.3 健康档案管理服务调用

POS系统应调用省级人口健康综合管理平台提供的健康档案管理服务，完成健康档案的文档注册、事件注册、索引管理及相关信息查询等功能。

机构不要将相关操作逻辑嵌入到机构POS系统的日常医疗业务流程中，即不要将操作成功与否作为日常医疗业务流程是否可继续流转的必要条件，而是作为一个单独的处理逻辑进行实时或异步调用，并根据省级人口健康综合管理平台的处理结果记录相关信息的操作状态，对操作不成功的信息应有自动或手动重新调用省级人口健康综合管理平台服务直至处理成功的功能，确保健康档案信息的完整性。

10.2.4 健康档案调阅服务调用

POS系统可根据省级人口健康综合管理平台分配的居民唯一标识ID查询并获取居民不同类型的健康档案文档，以实现健康档案的共享利用。

10.2.5 健康档案协同服务调用

医疗机构之间通过省级人口健康综合管理平台实现业务的协同，POS系统应实现省级人口健康综合管理平台提供的区域业务协同服务（例如专家远程咨询会诊、双向转诊等区域协同业务）的发起和受理功能，以满足区域业务协同的需要。

10.2.6 健康档案浏览器调用

机构可以在自己的各个POS服务系统中嵌入省级人口健康综合管理平台提供的健康档案浏览器，以便和自己的系统进行更好的整合，通过健康档案浏览器查看居民的健康档案信息。

10.2.7 安全与隐私服务调用

POS系统通过安全与隐私服务实现安全地提交和使用健康档案数据，参与医疗卫生业务协同。

10.3 信息服务接入规范

10.3.1 省属医院

表32 病历文档上传服务调用

服务序号	服务名称	服务描述
1	就诊记录文档上传服务调用	上传病人的自然信息和就诊信息，这些信息至少应包含个人ID、姓名、性别、出生日期、身份证号、出生地、职业、联系

		方式等，以及就诊医院、就诊科室、就诊时间、接诊医生等。
2	病案首页文档上传服务调用	病人整个住院过程中诊断、治疗、护理、费用开支等综合情况的反映，它的许多内容被临床研究、医院管理、医疗卫生统计、医疗纠纷处理及医疗付款等方面广泛利用，主要包含的内容有病人的自然信息和医疗信息。
3	手术记录文档上传服务调用	包括手术日期时间、术前诊断、术中诊断、手术名称、手术医师、麻醉方法及麻醉医师、手术经过包含内容、术者体位、消毒方法、切口部位等信息。
4	用药记录文档上传服务调用	病人就诊期间的药品处方、医嘱信息的上传，包括药品编码、药品名称、剂量、用法、开单医生、用药时间等信息。
5	非用药医嘱文档上传服务调用	病人就诊期间除药品外的所有医嘱信息的上传，包括护理医嘱、治疗医嘱、检查、检验、手术医嘱等。
6	检查报告文档上传服务调用	病人就诊期间所有检查报告上传。
7	检验报告文档上传服务调用	病人就诊期间所有检验报告上传。
8	体检记录上传服务调用	体检相关数据文档上传。
9	过敏记录上传服务调用	病人的过敏史、过敏源、过敏症状、过敏病情、过敏严重性等信息的上传。
10	临床摘要文档上传服务调用	病人就诊期间的临床摘要文档上传。
11	完整电子病历文档上传服务调用	一次性上传病人就诊期间产生的完整电子病历文档，用于批量文档上传。

表33　其他业务文档上传服务调用

服务序号	服务名称	服务描述
1	疾病预防控制信息上传服务调用	疾病预防控制中心要求医院上报的数据，包括免疫接种、传染病报告、结核病防治、艾滋病综合防治、血吸虫病病人管理、职业病报告、职业性健康监护、伤害监测报告、中毒报告、行为危险因素监测、死亡医学登记等。
2	儿童保健信息上传服务调用	主要包括出生医学证明、新生儿疾病筛查、出生缺陷监测、体弱儿童管理、儿童健康体检、儿童死亡管理等数据。
3	妇女保健信息上传服务调用	主要包括妇女婚前保健、计划生育、妇女病普查、孕产妇保健服务及高危管理、产前筛查与诊断、孕产妇死亡报告等数据。

表34　病历数据查询服务调用

服务序号	服务名称	服务描述

1	病案首页文档查询服务调用	根据个人 ID 等条件查询病案首页文档
2	手术记录文档查询服务调用	根据个人 ID 等条件查询手术记录
3	用药记录文档查询服务调用	根据个人 ID 等条件查询用药情况
4	非用药医嘱文档查询服务调用	根据个人 ID 等条件查询非用药医嘱
5	检查报告文档查询服务调用	根据个人 ID 等条件查询历次就诊检查报告
6	检验报告文档查询服务调用	根据个人 ID 等条件查询历次就诊检验报告
7	体检记录查询服务调用	根据个人 ID 等条件查询体检相关数据文档
8	过敏记录查询服务调用	根据个人 ID 等条件查询病人的过敏史、过敏源、过敏症状、过敏病情、过敏严重性等信息
9	临床摘要文档查询服务调用	根据个人 ID 等条件查询临床摘要文档
10	完整病历文档查询服务调用	根据个人 ID 等条件查询所有病历文档

10.3.2 市级区域卫生信息平台

表35 数据上传服务调用

服务序号	服务名称	服务描述
1	个案实时数据采集服务调用	根据个人 ID 等条件查询个人基本信息，平台上已注册的个人基本信息，可在该区域内的各医疗机构之间共享，任何一个授权的医疗机构都可以通过平台查询调用居民的个人基本信息。
2	批量数据采集服务	根据个人 ID 等条件查询居民主要疾病和健康问题摘要信息。
3	基于 XDS 数据采集服务调用	根据个人 ID 等条件查询儿童保健信息。

表36 数据查询服务调用

服务序号	服务名称	服务描述
1	个人基本信息查询服务调用	根据个人 ID 等条件查询个人基本信息。
2	医疗机构服务调用	根据医疗机构 ID 等条件查询医疗机构相关的信息。
3	医护人员服务调用	根据医护人员 ID 等条件查询医护人员相关的信息。
4	术语字典服务调用	根据值域或编码系统 ID 等条件查询相关术语信息，根据两个值域 ID 获取两者之间的映射信息。
5	共享文档查询服务调用	根据共享文档 ID 等条件查询共享文档相关信息。
6	综合管理数据查询服务调用	根据综合管理数据相关查询参数查询综合管理数据相关信息。

10.3.3 国家人口健康信息平台

表37 基础数据同步服务调用

服务序号	服务名称	服务描述
1	个人数据同步服务调用	使国家和省级平台之间的居民个人基本信息同步。

2	医疗机构数据同步服务调用	使国家和省级平台之间的医疗机构信息同步。
3	医护人员数据同步服务调用	使国家和省级平台之间的医护人员信息同步。
4	诊疗数据同步服务调用	使国家和省级平台之间的诊疗数据同步。
5	健康档案数据同步服务调用	使国家和省级平台之间的健康档案数据同步。

11 性能要求

系统建设时应满足业务开展要求和用户使用习惯的需要，在此基础上满足系统性能要求，系能要求的指数是在任何环境下必须达到的要求，具体指标要求如下：

11.1 最小并发用户数

对于省级人口健康综合管理平台的服务，

人口≤100万，允许每分钟最小并发用户数400个。

100万≤人口≤500万，允许每分钟最小并发用户数1800个。

11.2 基础服务平均响应时间

a) 患者注册服务调用，单个患者注册平均响应时间小于 1 秒；
b) 健康档案查询，按患者唯一标识查询，返回患者电子健康档案文档目录树时，平均响应时间小于 2 秒；
c) 患者基本信息查询，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；
d) 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。

11.3 健康档案交换服务性能

a) 单记录交换/入库的平均响应时间≤20ms；
b) 批量数据上传：峰值 800 笔/分钟。

11.4 健康档案调阅服务性能

a) 千万级数据量下单记录本地查询的响应时间≤2 秒；
b) 千万级数据量下分布式查询的响应时间≤5 秒/次。

11.5 健康档案协同服务性能

a) 健康档案协同服务响应：峰值 30 笔/秒；
b) 健康档案协同接受服务请求时间≤2 秒；
c) 健康档案协同发送业务服务时间≤5 秒；

11.6 统计分析性能

a) 简单统计报表查询：响应时间≤10 秒；
b) 千万级数据量下单项统计的响应时间≤5 秒；
c) 复合汇总统计响应时间≤120 秒；
d) 生成复杂统计报表的响应时间≤180 秒。

11.7 网络性能要求

a) 核心路由器性能要求：
- 支持分区供电，每路电源的电流不超过 100A
- 支持接口类型包括： 40GPOS、10GPOS、2.5GPOS、10GE、GE、FE、155M/622M ATM、CPOS、E1/T1、CE1
- 支持主控与转发相分离
- 支持主控、电源、风扇冗余
- 任意端口支持镜像，支持本地镜像和远程镜像功能
- 提供软件热补丁技术，实现设备软件完全平滑升级
- 支持基于状态的热备份切换，实现不间断路由转发，所有组件可热拔插

b) 核心交换机性能要求：
- 支持主控板堆叠，堆叠带宽>=160G
- 支持分区供电，颗粒化电源，支持 N+N 电源冗余（AC 和 DC 均支持）
- 支持风扇冗余，支持风扇模块分区管理，支持风扇自动调速
- 支持独立的硬件监控模块，支持电源监控
- 电源要求支持标准 SFP、XFP、SFP+模块
- 支持全分布式转发

c) 接入交换机性能要求：
- 端口类型需要支持百兆电口下行、千兆光口上行
- 防雷指标≥6KV
- 要求整机达全线速转发能力
- 电口和光口都支持端口休眠功能
- 支持堆叠，主机堆叠数不小于 9 台，堆叠带宽>=48G
- 接口模块要求支持标准 SFP、SFP+模块

d) 防火墙性能要求：
- 整机最大吞吐量 ≥ 80Gbit/s
- ACL 规则数 ≥ 12 万
- 并发连接数 ≥ 800 万
- 每秒新建连接数 ≥ 50 万
- VPN 性能 ≥ 12G
- IPSec 隧道数 ≥ 32 万
- L2TP 隧道数 ≥ 16G
- GRE 隧道数 ≥ 8000

e) 网络入侵检测设备性能要求：
- 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
- 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

附 录 A
（资料性附录）
服务点系统（POS）分类

服务点系统（POS）按照规模分为4种类型。

A.1 一类服务点系统（POS1）

POS1 特点：

- 病人流量大、医院规模大
- 地理位置距离数据中心较近
- 内部已有完善的业务系统，有自己的本地存储
- 终端主机日常访问本 POS 内的业务系统

POS1 类型：

- 市级二甲以上医院
- 市区内社区卫生服务中心
- 妇幼保健医院

A.2 二类服务点系统（POS2）

POS2 特点：

- 病人流量大、医院规模大
- 地理位置距离数据中心较远
- POS 内主机为单纯的门户，所有业务应用都依赖于远程的一个集中式的业务平台的支持，该业务平台位于上一级的管理机构，客户端既没有应用程序，也没有存储

POS2 类型：

- 市为单位建省级人口健康综合管理平台
- 区或县级所属的大中型医疗机构
- 区/县级医院
- 大型乡镇卫生院
- 偏远社区卫生服务中心

A.3 三类服务点系统（POS3）

POS3 特点：

- 病人流量小、医院规模小
- 地理位置距离数据中心较远
- POS 内工作站端实际上是一个包含业务应用程序和存储的完整系统

POS3 类型：

- 小型乡镇卫生院
- 社区卫生服务站
- 卫生室
- 个人移动办公

A.4 四类服务点系统（POS4）

POS4 特点：

- POS 内主机为单纯的 Portal
- 业务系统在信息平台内部

POS4 类型：

- 卫生室
- 个人