ICS 点击此处添加 ICS 号
点击此处添加中国标准文献分类号

WS

# 中 华 人 民 共 和 国 卫 生 行 业 标 准

WS/T XXXXX—2014

# 远程医疗信息系统技术规范

Technical specification for telemedicine information system

点击此处添加与国际标准一致性程度的标识

（征求意见稿）

（本稿完成日期：）

2014－XX－XX 发布　　2014－XX－XX 实施

中华人民共和国国家卫生和计划生育委员会
发 布

# 目　　次

# 前　言

本标准由国家卫生标准委员会信息标准专业委员会提出并归口。
本标准主要起草单位：
本标准主要起草人：

# 远程医疗信息系统技术规范

## 1 范围

本标准规定了远程医疗信息系统总体框架和技术架构、系统功能、信息资源规范、IT基础设施规范、安全规范和性能要求等。

## 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 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 第2部分 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 3304-1991 中国各民族名称的罗马字母拼写法和代码

GB/T 4658-1984 文化程度代码

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 22239-2008 信息安全技术 信息系统安全等级保护基本要求

WS 218-2002 卫生机构（组织）分类与代码

WS 363-2011 卫生信息数据元目录（所有部分）

WS 364-2011 卫生信息数据元值域代码（所有部分）

WS 445-2014 电子病历基本数据集（所有部分）

WS XXX-2014 卫生信息共享文档规范

WS/T XXX-2014 远程医疗信息系统基本功能规范

WS/T XXX-2014 基于电子病历的医院信息平台技术规范

ICD-9-CM-3 手术与操作

ICD-10 国际疾病分类

卫办发［2002］116号 医院信息系统基本功能规范

卫办综函［2010］1046号 2010年远程会诊系统建设项目管理方案

卫办综函［2011］102号 2010年远程医疗系统项目技术方案

## 3 术语和定义

WS/T XXX-2014 远程医疗信息系统基本功能规范的术语和定义适用于本规范。

## 4 缩略语

HIS：医院信息系统（Hospital Information System）
LED：发光二极管（Light Emitting Diode）
DICOM3.0：医学数字影像和通信标准（Digital Imaging and Communications in Medicine）
PACS：图像归档和通信系统（Picture Achieving and Communication System）
PC：个人计算机（Personal Computer）
EMR：电子病历（Electronic Medical Record）
EHR：电子健康档案（Electronic Health Record）
3G：第三代移动通信系统(The Third Generation)
AAC-LD：高级音频编码低时延(Advanced Audio Coding with Low Delay)
ABR：区域边界路由器(Area Border Router)
AD：目录服务器(Active Directory)
ADSL：非对称数字用户线路(Asymmetric Digital Subscriber Line)
AE：自动曝光(Automatic Exposure)
AEC：多路回声抵消(Acoustic Echo Cancellation)
AF：自动聚焦(Automatic Focus)
AGC：自动增益控制(Automatic Gain Control)
ALG：应用层网关(Application Level Gateway)
ANS：自动噪音抑制(Automatic Noise Suppression)
APN：接入点名称(Access Point Name)
AS：自治系统(Autonomous System)
AWB：自动白平衡(Automatic White Balance)
BE：数据节点(Back End)
BFCP：资源管理协议（Binary Floor Control Protocol）
BFD：双向转发检测(Bidirectional Forwarding)
BGP：边界网关协议(Border Gateway Protocol)
CCD：电荷耦合器件(Charge Coupled Device)
CDR：话单(Call Detail Record)
CIDR：无类别域间路由(Classless Inter-Domain Routing)
CIF：标准图像格式，支持352×288分辨率(Common Intermediate Format)
CoS：服务等级(Class of Service)
CPU：中央处理器(Central Processing Unit)
CVBS：复合视频基带信号(Composite Video Base Signal)
DDoS：分布式拒绝服务(Distributed Denial of Service)
Diff-Serv：有差别服务(Differentiated Service)
DMZ：半信任区(Demilitarized Zone)
DNS：域名服务器(Domain Name Server)
DSCP：差分服务码点(Differentiated Services Code)
DVI：数字显示接口(Digital Visual Interface)
EGP：外部网关协议(Exterior Gateway Protocol)
EMC：电磁兼容性(ElectroMagnetic Compatibility)
EXP：实验比特位(Experimental Bits)
FCoE：以太网光纤通道(Fibre Channel over Ethernet)
FCP：光纤通道协议(Fibre Channel Protocol)

FRR: 快速重路由(Fast Reroute)
FTP: 文件传输协议(File Transfer Protocol)
GK: 网守(Gatekeeper)
GR: 优雅重启(Graceful Restart)
GW: 网关(Gate Way)
H.264 Basic Profile：H.264基本画质编码算法
H.264 High Profile：H.264高级画质编码算法
H.264 SVC：H.264可分级编码
H.460：用于音视频的网络穿越的协议
HA: 高可靠性(High Availability)
HDMI: 高清晰多媒体接口(High Definition Multimedia Interface)
H-QoS: 层次化QoS(Hierarchical Quality of Service)
HTTP: 超文本传输协议(Hypertext Transfer Protocol)
HTTPS: 超文本传输安全协议(Hypertext Transfer Protocol Secure)
ICMP: 因特网控制报文协议(Internet Control Message Protocol)
IDS: 入侵检测系统(Intrusion Detection System)
IGP: 内部网关协议(Interior Gateway Protocol)
IMS: IP多媒体子系统(IP Multimedia Subsystem)
IOPS: 每秒进行读写操作的次数(Input/Output Operations per Second)
IP: 互联网协议(Internet Protocol)
IPS: 入侵防御系统(Intrusion Prevention System)
IPsec: 因特网协议安全协议(Internet Protocol Security)
iSCSI: 因特网小型计算机系统接口(Internet SCSI)
ISDN: 综合业务数字网(Integrated Services Digital Network)
IS-IS: 中间系统到中间系统(Intermediate System to Intermediate System)
ISP: 因特网服务提供方(Internet Service Provider)
I-SPF: 增量路由计算(Incremental Shortest Path First)
ITU: 国际电信联盟(International Telecommunications Union)
ITU-T: 国际电信联盟－电信部分(International Telecommunications Union-Telecommunication)
IVR: 互动式语音应答(Interactive Voice Response)
LCD: 液晶显示器(Liquid Crystal Display)
LDAP: 轻型目录访问协议(Lightweight Directory Access Protocol)
LSA: 链路状态公告(Link State Advertisement)
LUN: 逻辑单元号(Logical Unit Number)
MAC: 消息鉴别码(Message Authentication Code)
MC: 多点控制器(Multipoint Controller)
MCU: 多点控制单元(Multipoint Control Unit)
MP: 多点处理器(Multipoint Processor)
MPLS: 多协议标记交换(Multiprotocol Label Switching)
MTBF: 平均故障间隔时间(Mean Time Between Failures)
MTTR: 平均修复时间(Mean Time to Repair)
NAT: 网络地址转换(Network Address Translation)

NBU: 网络备份服务器(NetBackup)
NDMP: 网络数据管理协议(Network Data Management Protocol)
NGN: 下一代网络(Next Generation Network)
NSR: 不间断路由(Non-Stop Routing)
OA: 办公自动化(Office Automation)
OSPF: 开放式最短路径优先(Open Shortest Path First)
PHB: 逐跳行为(per-hop behavior)
PoE: 以太网供电(Power Over Ethernet)
PRC: 部分路由计算(Partial Route Calculation)
PSTN: 公用交换电话网(Public Switched Telephone Network)
QoS: 服务质量(Quality Of Service)
RADIUS: 一种远程AAA拨号服务(Remote Authentication Dial-In User Service)
RAID: 独立磁盘冗余阵列(Redundant Array of Independent Disks)
RIP: 路由信息协议(Routing Information Protocol)
RP: 路由执行器(Route Processor)
RPO: 以恢复点为目标(Recovery Point Objective)
RTCP: 实时传输控制协议(Real-time Transfer Control Protocol)
RTP: 实时传输协议(Real-time Transfer Protocol)
SAS: 串行连接的SCSI(serial attached SCSI)
SATA: 串行的ATA(Serial Advanced Technology Attachment)
SCSI: 小型计算机系统接口(Small Computer System Interface)
SDH: 同步数字体系(Synchronous Digital Hierarchy)
SEC: 超强纠错(Supper Error Concealment)
SLA: 服务水平协议(Service Level Agreement)
SMC: 业务管理中心(Service Management Center)
SMI-S: 存储管理主动规范(Storage Management Initiative – Specification)
SNMP: 简单网络管理协议(Simple Network Management)
SOAP:简单对象访问协议(Simple Object Access Protocol)
SPC: 存储程序控制(Stored Program Control)
SPI: 同步并行接口(Synchronous Parallel Interface)
SRTP：安全实时传输协议(Secure Real-time Transport Protocol)
SSD: 固态磁盘(Solid-State Drive)
SSH: 安全外壳(Secure Shell)
SSL: 安全套接层(Secure Sockets Layer)
TCP: 传输控制协议(Transmission Control Protocol)
TE: 远程呈现终端(Telepresence Endpoint)
TLS: 传输层安全(Transport Layer Security)
UCD: 用户为中心的设计(User Centered Design)
UDP: 用户数据报协议(User Datagram Protocol)
VGA: 视频图形阵列(Video Graphics Array)
VME: 活动视频增强(Video Motion Enhancement)
VoD: 视频点播(Video on Demand)
VoIP: 基于IP的语音传输(Voice over Internet Protocol)

VOIP GW: 宽带语音网关(Voice over Internet Protocol Gate Way)
VPN: 虚拟专用网(Virtual Private Network)
VRRP: 虚拟路由冗余协议(Virtual Router Redundancy Protocol)
VSS: 虚拟软件交换机(Virtual Software Switch)
WAN: 广域网(Wide Area Network)
XML: 可扩展标记语言(Extensible Markup Language)

## 5 软件技术总体要求

### 5.1 总体框架

远程医疗信息系统总体框架主要包括远程医疗信息系统的应用、远程医疗信息系统服务、信息资源中心、信息交换层、基础措施、标准规范体系、安全保障体系，见图1。


图1 远程医疗信息系统总体框架

### 5.2 技术架构

本规范中的远程医疗信息系统技术架构如下图所示：

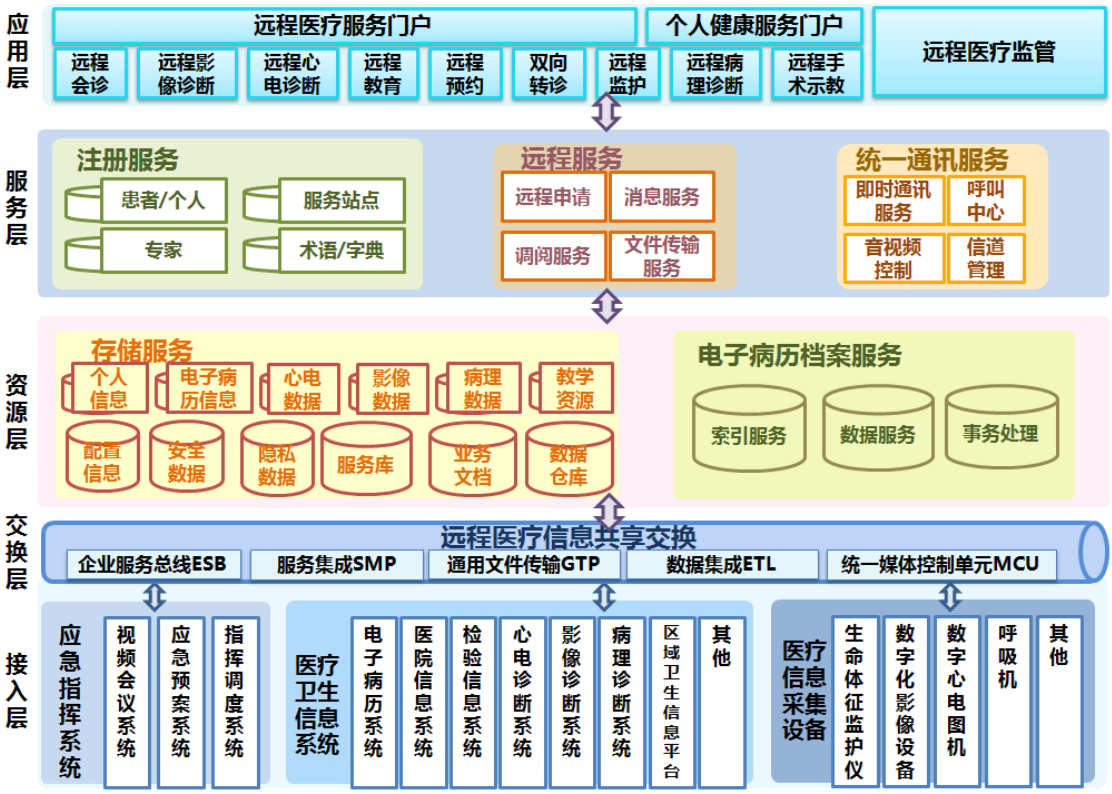


图2　远程医疗信息系统技术架构

### 5.2.1　应用层

远程医疗信息系统应用层由远程医疗服务应用和远程医疗监管2部分（模块）组成；通过统一的远程医疗服务门户访问，可实现远程会诊、远程影像诊断、远程病历诊断、远程心电诊断、远程监护、远程手术示教、远程医学教育等远程医疗服务，各应用可实现“即插即用”；通过远程医疗监管模块提供的功能，可实现各级远程医疗系统运营情况的分析、统计、决策等多种监管功能。

### 5.2.2　服务层

远程医疗信息系统服务层所提供的服务包括注册服务、远程服务、存储服务和电子病历档案服务，用于通过远程医疗数据传输对象与远程医疗业务逻辑层直接进行交互，集中了系统的业务逻辑的处理。服务间的消息交换和消息传输贯穿各个服务层，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。

### 5.2.3　资源层

远程医疗信息系统资源层所提供资源包括结构化数据、非结构化（文档、音视频资料）数据、结构化文档数据、应用服务资源等。主要用于支撑跨区域远程医疗工作开展的管理协调；支撑跨区域远程医疗工作开展的效能建设；辅助决策开展数据统计分析服务；为国家远程医疗监管与资源服务中心与各区域远程医疗监管与资源服务中心，以及各区域远程医疗监管与资源服务中心之间的互联互通提供信息服务。

### 5.2.4　交换层

远程医疗信息资源交换层包括：企业服务总线ESB、服务集成SMP、通用文件传输GTP、数据集成ETL、统一媒体控制单元MCU。信息交换层根据业务流程，通过数据接口或消息传递与其他信息系统进行数据交换，实现信息共享、数据上报等功能。主要用于满足临床信息跨医院、跨区域的信息交换和协同应用；用于医疗服务资源的注册、申请、授权、管理、监控，实现基于服务的信息资源共享交换；用于满足基于卫生医疗行业数据规范的业务信息采集，并对外部系统提供基于文件的数据交换服务；用于满足远程医疗数据仓库建设过程中的数据采集、加工、转换处理的数据集成要求；用于满足音视频信息的跨医院、跨区域交互，并按照平战结合要求，集成突发公共卫生事件应急指挥视频会议系统。解决医院依靠区域远程医疗监管与资源服务中心开展远程医疗业务过程中的信息互联互通问题。

#### 5.2.5 接入层

远程医疗信息资源接入层是远程医疗系统的基础，包括三大类：应急指挥系统、医疗卫生信息系统及医疗信息采集设备。

##### 5.2.5.1 应急指挥系统

远程医疗信息系统与应急指挥系统对接，利用视频站点连接医院网络，提供现场和救治过程音视频动态信息，实现突发事件应对中的信息共享与处置联动，既可使患者通过远程视频获得诊治，也可助医护人员随时向指挥中心汇报患者的最新情况，分析任何潜在的新疾病。

##### 5.2.5.2 医疗卫生信息系统

主要包括电子病历系统、医院信息系统、检验信息系统、临床信息系统、心电诊断系统、影像诊断系统、病理诊断系统和其他医疗信息系统。通过远程医疗信息系统与医疗信息系统的对接，实现跨医院之间的信息共享、业务协同。

远程医疗信息系统与区域卫生信息平台对接，提供远程医疗监管与业务服务实时信息，共享原有健康档案和电子病历信息，使区域卫生信息平台具有对远程医疗业务的综合管理功能。

如医疗机构已经建立了数据共享的医院信息集成平台，将通过平台机制，实现与远程医疗信息系统的对接，减少数据接口数量，实现跨医院之间的信息共享、业务协同。

##### 5.2.5.3 医疗信息采集设备

医疗信息采集设备主要包括多参数生命体征监护仪、数字化影像设备、数字心电图机、呼吸机和其他医疗信息采集设备，主要用于采集患者的生命体征、血糖、血压等数据。

#### 5.2.6 远程医疗服务门户

远程医疗服务门户用于宣传远程医疗资源、案例分享、外网远程申请，方便查看最新远程医疗咨询和动态，主要包括远程会诊门户、远程教育门户等。

### 5.3 软件架构要求

基本要求包括：

——远程医疗信息系统软件架构应该基于面向服务架构的思想来构建；系统采用 B/S 模式结构，根据应用环境的不同，以网络最优化方案进行系统部署；

——符合已有的标准框架协议，采用业界协议；采用开放式标准设计，能够兼容其他医疗系统和设备；满足今后的发展，为未来业务扩展留有充分的扩充余地；

——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；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；

——远程医疗信息系统要求具有消息路由功能，可以具有业务流程管理（BPM）、可以支持远程医疗业务流程编排和人工参与的工作流。

### 5.4 软件技术要求

#### 5.4.1 基本要求

基本要求包括：

——系统应支持远程医疗服务相关的业务操作，可具有支持业务流程编排的功能；

——系统应支持与各医院信息系统的信息共享和交互，具有医疗信息和资料调阅功能；

——系统应提供管理工具，能够管理所有业务系统集成节点，监控整个远程医疗业务开展情况；

——系统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，系统日志的记录与查看，支持消息可靠性传递及消息追踪等；系统具有很好的备份功能，满足高可靠性需求；

——单点登录：提供对各种应用系统和数据的安全集成，用户只需登录一次就可以访问其它应用系统和数据库；

——远程医疗信息系统，应提供二次开发环境，提供基础公共业务组件的封装。

#### 5.4.2 交互信息要求

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

### 5.5 集成能力要求

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。具体要求包括：

——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；

——系统应支持主流的卫生信息交换国际标准和规范；

——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。

## 6 系统功能

### 6.1 基础功能

#### 6.1.1 基本要求

基础功能应包括对患者、医疗服务人员、医疗机构（科室）、医疗卫生术语的注册管理服务。系统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），各注册库具有管理和解决单个实体具有多个标识符问题的能力。

#### 6.1.2 个人注册服务

个人注册服务是用于对申请远程医疗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，可以为远程医疗信息系统上的各应用系统提供一致的个人信息。基本功能包括：

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

### 6.1.3 卫生人员注册服务

医疗卫生人员注册服务是用于对医疗机构内部所有医疗卫生人员的基本信息进行注册和管理。医疗卫生人员包括医生、护士、医技人员、医院管理员、科室管理员等全部提供医疗卫生服务的医务人员。通过对医疗人员基本信息、专业信息的管理，可以在远程医疗信息系统上的各应用系统，提供完整、统一的医疗人员信息。基本功能包括：

——具备新增医疗卫生人员注册功能；
——具备医疗卫生人员信息更新功能；
——具备医疗卫生人员身份失效功能
——具备医疗卫生人员身份合并功能；
——具备医疗卫生人员信息查询功能。

### 6.1.4 医疗机构（科室）注册

医疗机构（科室）注册是用于对医疗机构（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，可以为远程医疗信息系统上的各应用系统、患者提供完整、统一的医疗机构科室信息。基本功能包括：

——具备新增医疗机构（科室）注册功能；
——具备医疗机构（科室）信息更新功能；
——具备医疗机构（科室）停用功能；
——具备医疗机构（科室）信息查询功能。

### 6.1.5 代码字典注册

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

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

## 6.2 远程医疗数据资料整合功能

### 6.2.1 上传功能

可以支持数据资料的批量上传和个案数据资料实时上传。

支持按DICOM标准获取患者的影像资料，并进行存储、再现以及相应的后处理操作。

支持将病理切片转换成由完整数字图像组成的虚拟数字切片，至少包括20倍和40倍显微图像。支持病理虚拟数字切片上传。

支持从电生理检查设备采集电生理数据，并进行无损的数据传输、存储和再现。电生理图支持通过Internet、GPRS、电话线等方式传输电生理检查数据。电生理图数据可存储为XML、DICOM等通用数据格式。

支持床边监护仪等生命体征数据的实时传输。

#### 6.2.2 复制功能

在现有的远程医疗的应用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。

#### 6.2.3 数据质量控制功能

用于跟踪和监控远程医疗信息系统里的数据质量。

在本规范中暂不规定与数据质量控制相关服务和接口。

#### 6.2.4 申请功能

申请功能是远程医疗信息系统在电子申请单处理过程中（远程会诊申请单、远程转诊申请单、远程预约申请单等）为平台上的各应用系统提供申请单信息共享服务。基本功能包括：

——具备申请单接收功能；

——具备申请单查询功能。

### 6.3 远程医疗数据资料存储服务功能

远程医疗数据中心作为远程医疗信息系统的中枢，实现各类远程医疗数据的存储和管理，并为远程医疗各应用系统等提供数据挖掘和分析支持。

远程医疗数据资料存储服务是一系列存储库，用于存储远程患者病例资料。根据远程医疗病例资料信息的分类，存储服务可包括六个存储库：个人基本信息存储库、电子病历信息存储库、健康档案信息存储库、会诊信息存储库、影像数据存储库、教学资源存储库。

用于接收电子病历文档、影像、视频资料,并将文档注册到索引服务中，同时对文档的版本及生命周期管理，它还提供文档接收服务。基本功能包括：

——具备接收文档、影像、视频数据资料功能；

——具备向索引库注册文档、影像、视频数据资料功能；

——具备向使用者提供文档、影像、视频数据资料功能。

### 6.4 远程医疗数据资料管理功能

#### 6.4.1 数据资料管理功能

对患者全病程档案进行管理，包括建档、注销、属地变更等。

#### 6.4.2 文档注册功能

文档注册根据文档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的地址。文档注册可根据文档用户的特定查询条件返回文档（集）。

#### 6.4.3 事件注册功能

为实现远程医疗信息系统对病例资料信息的共享和交换，需要以远程医疗患者为单位，对患者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。

#### 6.4.4 索引服务功能

远程医疗信息系统用户在被授权的情况下，可以通过索引服务从POS系统查看某患者的病例资料信息，以及事件信息所涉及的文档目录及摘要信息。再结合远程病例资料存储服务可以实现文档信息的即时展示，使用户更多的了解患者既往的健康情况。

索引服务全面掌握远程医疗信息系统所有关于患者的诊疗信息事件，包括患者的就诊时间、科室、接受的医疗服务、产生文档（医疗记录）。通过索引服务可以查看某患者的诊疗事件信息，以及事件信息所涉及的文档目录及摘要信息。基本功能包括：

——具备静态文档注册功能；

——支持根据医疗事件或患者信息查询相关医疗静态文档索引的功能。

### 6.5 远程医疗数据资料调阅功能

用于对文档、影像图片、病历文件等各类数据的浏览查阅。

#### 6.5.1 组装服务功能

组装服务通过调用不同的系统组件生成多个患者数据的结果集，并把这些结果集组合成一定输出格式。

#### 6.5.2 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。

#### 6.5.3 数据访问服务功能

数据访问服务提供对单个患者病例资料文档或文档集的数据的查询和访问服务。

### 6.6 远程医疗结果信息反馈功能

结果信息反馈功能是远程医疗信息系统在远程诊疗过程中对远程诊疗结果信息共享服务。基本功能包括：

——具备结果信息接收功能；

——具备结果信息查询功能。

### 6.7 远程即时通讯功能

远程视音频通讯功能需遵从H.323、SIP基本视频通讯协议实现。 系统需具备视讯业务管理功能、视频多点交换单元功能、音视频接入单元功能、录播功能。

#### 6.7.1 视讯业务管理功能

视讯业务管理功能是会议调度、会议管理、网络管理、资源管理等一系列模块的总和。其主要功能是实现对视讯网络的统一控制、统一资源调度和管理，同时通过与视讯交换设备的交互，完成对视讯业务全流程的控制和管理。

业务管理系统必须能够支持管理员预约和终端自主召集会议，能够管理标清、高清MCU，能够召开和控制标清、高清、高标清混合会议和智真多点会议，能够自动召开二级级联会议，并支持手动多级级联，支持多通道级联会议调度。必须支持网内设备注册管理，最大支持不少于1000点，实现地址解析、接入控制、带宽管理功能。支持公私网穿越组网的实现。必须支持标准的第三方接口，接口规范遵从《远程医疗信息系统交互规范》要求。

### 6.7.2 视频多点交换功能

视频多点交换功能由多点控制单元（MCU）实现，是视讯会议业务的汇接处理设备，从逻辑上分为多点控制器（MC）和多点处理器（MP），MC提供了多方视讯会议的呼叫建立和控制功能，MC的控制功能通过H.245来完成。MP在多方视讯会议中，接收来自终端或级联MCU、GW的音频、视频和数据流，处理这些媒体流并把它们送回到终端、MCU或GW。

MCU必须支持标清、高清、高标清混合会议和智真多点会议，必须支持多画面、速率适配协议适配，必须支持视音频抗丢包和自动带宽控制，必须支持3级以上级联和多通道级联，必须支持业务备份和线路备份，支持主备倒换。

### 6.7.3 音视频接入功能

音视频接入功能由视讯终端实现，是视讯会议业务的用户侧设备，主要提供功能为：会议的呼叫建立和释放；会场图象和语音的采集与编码、对接收的图像和语音媒体流进行拆包、解码和输出；以及会议控制等功能。

视讯终端的会议控制功能，必须支持主席控制和语音激励两种控制方式。在会议的召开过程中，会议中的任何一个终端都具有查询会场列表、申请发言、申请主席等功能。当其通过申请成为主席后，必须具有以下主席控制功能，具体包括：会场浏览、增加和删除会场、多画面控制、广播会场、声音控制（闭音、静音等）、语音激励、点名发言、摄像机远遥、结束会议、释放主席等功能。

此外，视讯终端还必须能够支持通过主叫呼集自主召集会议，支持画中画、多画面显示，支持统一地址本。支持视音频抗丢包和线路备份功能。

### 6.7.4 录播功能

录播功能必须支持将会议中的视频、音频信号和医疗数据信息进行一体化的同步录制、直播和点播。视频录制系统基于IP网络，支持IPV4和IPV6双协议栈，支持IPv4单独组网、IPv6单独组网或者IPv4/IPv6混合组网，以满足网络发展需求。

## 6.8 远程医疗设备数据通讯功能

集成移动通信传输模块和传感信息接收模块的智能化、可视化和触摸式家庭智能健康终端设备。

自适应多信道信息传送机制和多样化的健康信息传感采集接入（如：蓝牙、WIFI、RFID接入、zigbee接入），支持和第三方健康生理指标检测仪进行zigbee自组网和数据传输功能，具有智能化、可视化、触摸式功能。

## 6.9 信息安全及隐私保护功能

### 6.9.1 用户管理及授权服务

远程医疗信息系统应为各应用系统提供统一的用户授权管理服务。基本功能包括：

——具备用户角色创建功能；

——具备用户授权功能；

——具备访问规则定制功能，并按规则访问数据的功能；
——具备记录用户权限操作日志功能。

#### 6.9.2 信息安全服务

远程医疗信息系统应提供统一的信息安全服务，用户在信息交互时系统通过认证等方式保证信息安全。

#### 6.9.3 隐私保护服务

远程医疗信息系统应提供患者隐私数据保护服务。

#### 6.9.4 审计追踪服务

远程医疗信息系统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。

## 7 信息资源规范

### 7.1 基础信息库

#### 7.1.1 基本要求

远程医疗信息系统的基础信息库包括患者基本信息、医疗卫生服务人员信息、医疗机构（科室）信息、术语和字典信息。基础信息库由远程医疗信息系统的注册服务产生，为这些实体提供统一、完整、准确的基本信息，并为这些实体提供唯一的标识。

#### 7.1.2 患者基本信息库

患者基本信息遵循WS 445-2014，应包括服务对象标识、人口学、联系人、地址、通信、医保等数据元。

#### 7.1.3 医疗卫生服务人员信息库

医疗卫生服务人员注册信息遵循WS 445-2014，应包括卫生服务者数据元。

#### 7.1.4 医疗卫生机构（科室）信息库

医疗机构（科室）信息遵循WS 445-2014，应包括卫生服务机构数据元。

#### 7.1.5 术语和字典库

远程医疗信息系统的术语和字典库遵循WS 363-2011、WS 364-2011、WS 445-2014等国家颁布的相关卫生数据标准，参考国际卫生行业相关数据标准。

### 7.2 远程医疗数据资料库

#### 7.2.1 文档存储库

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

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

共享文档包括病历概要、检查记录、检验记录、治疗记录、一般手术记录、输血记录、一般护理记录、病重（病危）护理记录、手术护理记录、出入量记录、入院记录、首次病程记录、日常病程记录、住院医嘱、生命体征测量记录、会诊记录、转诊记录。

#### 7.2.2 影像存储库

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

#### 7.2.3 视频存储库

视频存储库（包括图像存储与后处理，病例库的报告及管理）必须完全基于WEB架构，以方便日后维护及远程教育。

在数据管理方面应具备较大的伸缩性，它可以集中管理远程教育工程中的所有素材，也可以将素材按类型或按学科划分开来，单独进行管理，可将大素材库切分为多个小素材库。

#### 7.2.4 文档注册库

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

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。

## 8 IT基础设施规范

### 8.1 基本要求

遵循《基于电子病历的医院信息平台技术规范》8.1。

### 8.2 基础软件

遵循《基于电子病历的医院信息平台技术规范》8.2。

### 8.3 硬件服务器

遵循《基于电子病历的医院信息平台技术规范》8.3。

### 8.4 存储系统

#### 8.4.1 基本要求

遵循《基于电子病历的医院信息平台技术规范》8.4.1。

#### 8.4.2 存储可靠性要求

遵循《基于电子病历的医院信息平台技术规范》8.4.2。

### 8.4.3 存储易管理性要求

遵循《基于电子病历的医院信息平台技术规范》8.4.3。

### 8.4.4 存储架构

#### 8.4.4.1 协议支持

——框架协议应支持 SCSI、SAS；
——映射层协议应支持 iSCSI、FCP、FC-SW、FC-PH、FC-PI、FCOE；
——接口协议应支持 SATA、SAS、SPC、SPI、SES；
——数据通信协议应支持 Telnet、SNMP、FTP、HTTP、HTTPS、SSH；
——互联网协议应支持 IPV6。

#### 8.4.4.2 接口支持

——支持 8Gbps FC；
——支持 1Gbps iSCSI；
——支持 10Gbps iSCSI；
——支持 SAS2.0 的磁盘通道；
——支持 SSD,SATA,SAS,NL-SAS 中的 3 种类型以上硬盘（需要提供原厂商官方网站截图证明）。

#### 8.4.4.3 设备组网

——支持 IP SAN 组网，最大支持 256 台主机连接；
——支持 FC SAN 组网，最大支持 4096 台主机连接；
——支持 FC 与 IP 混合组网，最大支持 4096 台主机连接；
——支持 FCOE 组网；
——支持双控双活。

#### 8.4.4.4 操作系统

——兼容 windows、Linux、MacOS X 等操作系统；
——支持 IBM AIX，HP-UX, Windows 等操作系统，支持配置 Unix、windows、linux 操作系统的多路径负载均衡软件。

#### 8.4.4.5 准入认证

——拥有自主知识产权，具有软硬件自主研发能力，保障后续产品的连续性；
——通过 CCC、CE、CB、REACH、ROHS 等国内及国际认证，并获得《中国环境标志产品认证证书》，存储设备制造商应通过 ISO9001 认证；
——获得 vSphere 5.0 VAAI、Vmware SRM 5.0 和 SMI-S v1.4 或以上版本的 CTP 认证，并提供官方证明。

#### 8.4.4.6 分级存储

——支持 SAS、SATA、SSD 等硬盘分级存储，能够智能识别系统热点数据，并自动复制到在 SSD 硬盘，以提高系统效率；
——Cache 预取提升持续数据业务的性能；
——Cache 镜像实现控制器之间的 Cache 数据互备。

#### 8.4.4.7 存储管理

——支持快照、镜像、复制、自动精简配置、Flash 缓存等；
——支持虚拟快照，支持对源 LUN 提供某一时间点的一致性可用虚拟副本，对同一源 LUN 支持最多 256 个快照，系统支持对 1024 个源 LUN 进行快照，系统在一阵列上最多可创建 2048 个快照；
——支持 LUN 拷贝（HyperCopy），支持阵列内、阵列间（同构与异构）的数据备份与迁移在一阵列上最多可创建 256 个 lun 拷贝（包括全量或增量），最多双控 32 个 LUN 拷贝（16 个/控制器）同时进行，每个源 LUN 最多 128 个目标 LUN；
——支持分裂镜像（HyperClone），支持为 LUN 建立的某时刻的完整的物理拷贝，实体快照；
——支持远程异步复制（HyperMirror/A），支持同构阵列间 IP/FC 远程异步容灾，在一个阵列上最多可创建 128 个异步远程镜像对，只能 1 个源 LUN 对 1 个目标 LUN，最大可连接 32 个远端阵列；
——支持远程同步复制（HyperMirror/S），支持同构阵列间 IP/FC 远程同步容灾，在一个阵列上最多可创建 256 个同步远程镜像对，最多 1 个源 LUN 对 2 个目标 LUN，最大可连接 32 个远端阵列；
——支持 HostAgent 主机代理；
——支持自动精简配置；
——支持 VSS、NBU、BE 调用阵列快照完成 Server-Free 备份；
——支持硬盘健康检测功能；
——支持按法规提供只读模式的 LUN；
——支持不小于 250 个连接主机的 License；
——支持图形化的管理软件，包括：盘阵，卷管理软件。配置存储服务器的图形化管理配置和监控软件。
——支持通过多路径实现控制器间的静态负载均衡与控制器内的动态负载均衡 ；
——支持在线 LUN 扩展，支持各个 LUN 自由合并以实现 LUN 的扩展，可跨越 RAID 组、RAID 级别进行 LUN 扩展
——支持 SSD/NL-SAS/SATA/SAS 硬盘框间混插。

#### 8.4.4.8 存储性能

——支持的最大带宽不小于 1GB /s；
——支持的最大 IOPS 不小于 100 万。

### 8.4.5 存储容量

——支持远程专科会诊数据保存 15 年；
——支持远程会诊过程数据保存 15 年；
——支持示教视频录制时长大于 1000 小时；
——支持视频会议录制时长大于 100 小时。

### 8.4.6 存储可靠性

#### 8.4.6.1 RAID

——支持硬件 RAID，支持 RAID 0、RAID 1、RAID3、RAID 10、RAID 5、RAID6 等；
——支持在线 RAID 容量扩展；
——支持硬盘框掉电、级联线路故障等恢复后 RAID 配置不丢失。

#### 8.4.6.2 热插拔

——支持控制器、电源、风扇、电池、硬盘、IO 模块等部件热插拔。

#### 8.4.6.3 冗余

——支持冗余电源、风扇、控制器、缓存断电保护功能；
——支持通过多路径软件的冗余路径。

#### 8.4.6.4 备份

——支持全局热备盘、硬盘预拷贝、数据保险箱、智能风扇调速、硬盘坏道智能修复、SATA 盘双通道；
——支持数据的自动备份、归档。

#### 8.4.6.5 可靠性指标

——系统可靠性不小于 99.999%；
——MTBF 不小于 700，000 小时；
——MTTR 不大于 2 小时。

#### 8.4.6.6 其他可靠性技术

——支持周期性的对硬盘进行扫描，发现硬盘故障启动智能修复程序与告警，将故障区域隔离；
——支持远程复制、远程镜像等保护技术，实现 RPO=0 数据不丢失；
——支持智能化硬盘加电技术，即硬盘缓上电技术，避免大量硬盘同时上电时，引起电流过载，跳闸风险。

### 8.4.7 存储安全

——支持用户鉴权；
——支持在用户多次登录失败时锁定该用户，使他在一定时间内不能登录；
——支持用户级别划分，可划分为超级用户、管理员用户、浏览用户；
——支持登陆方式的命令行采用 SSH 加密，WEB 采用 HTTPS 加密；
——主机鉴权支持 iSCSI CHAP 认证。

### 8.4.8 存储维护管理

——支持存储系统统一管理软件，支持 SMI-S 管理标准；
——支持通过命令行提供设备管理、业务管理、故障管理、性能监控等功能；
——支持远程下电，一键式升级；
——支持通过 SNMP 协议向 I2000 或第三方网管系统上报状态信息，告警信息；
——支持声光告警、邮件告警、短消息告警、日志记录；
——支持通过系统维护界面进行性能数据的统计；
——支持在创建 LUN 之后可以立即部署业务，无需等待格式化完成。

### 8.4.9 存储备份

#### 8.4.9.1 系统架构

——支持 VTL 引擎和存储单元的架构分离；

——支持 Active-Active 双引擎。

#### 8.4.9.2 系统接口

——支持 FC 端口；
——支持 iSCSI 端口。

#### 8.4.9.3 功能特性

——支持磁带归档功能，支持根据策略导出虚拟带库数据到物理带库,实现数据归档；
——支持远程复制；
——支持磁带加密；
——支持 Hosted Backup，可以集成备份软件，虚拟带库和磁带机可用于本地系统，从而不必使用专用备份服务器；
——支持 OpenStorage，统一管理备份软件和 VTL；
——支持 NDMP V2, V3, V4；
——支持按需增容，虚拟磁带的容量可以一次到位的设定为相应规格的容量，也可以设定初始的使用容量，然后设定当初始容量不够时每一次的数据增量，充分利用存储空间，避免空间闲置导致的空间浪费；
——支持重复数据删除；
——支持图形化管理界面，支持远程管理功能。

#### 8.4.9.4 虚拟能力

——支持虚拟 Quantum、HP、Sun、IBM 等主流厂家的数十种主流磁带库和磁带机；
——支持主流厂商带库，支持 HP、IBM LTO-1，2，3，4，5 等主流厂商带机；
——最大虚拟磁带库数量不小于 256；
——最大虚拟带机数量不小于 2048；
——最大虚拟磁带数量不小于 131070。

#### 8.4.9.5 备份性能

——备份速率不小于 2500 MB/S；
——最大并发流不小于 64。

#### 8.4.9.6 可靠性

——支持保险箱盘、全局热备盘；
——支持配置 2 套冗余存储单元，每套存储单元包括双控制器、冗余电源、冗余风扇；
——支持 CACHE 数据保护机制，支持全局热备盘和热备盘漫游；
——支持智能磁盘休眠技术。

### 8.4.10 存储配置要求

#### 8.4.10.1 中小型医院

远程医疗信息系统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：

——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 Windows、Linux、Unix 等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）。

——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。

——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≥75TB，最多支持存储容量≥200TB；
- 支持 LTO3\LTO4\LTO5 驱动器。

#### 8.4.10.2 大型三甲医院

远程医疗信息系统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：

——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 Windows、Linux、Unix 等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）。

——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。

——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≥120TB，最多支持存储容量≥400TB；
- 支持 LTO3\LTO4\LTO5 驱动器。

### 8.5 网络

稳定、可靠的网络支撑平台是远程会诊业务开展的必要保证。远程医疗业务开展过程中具有参与会诊的医院分布范围广，数据传输量大、交换频繁、呈现效果要求高、网络承载压力大等特点。因此远程医疗信息系统在网络设计构建中，要采用以下建网原则：

——高可靠性:网络系统的稳定可靠是应用系统正常运行的关键保证，在网络设计中应选用已规模商用的高可靠性网络产品，合理设计网络架构，制订可靠的网络备份策略，保证网络具有故障自愈的能力，最大限度地支持系统的正常运行。

——标准开放性:支持国际上通用标准的网络协议（如 TCP/IP）、国际标准的大型的动态路由协议（如 BGP、ISIS）等开放协议，有利于以保证与其它网络之间的平滑连接互通，以及将来网络的扩展。

——安全性:通过设备机制及组网方案提高网络整体的安全性，对于所承载的各种增值类业务，要能提供类似于传统专线一样的安全性。

——灵活性及可扩展性:根据未来业务的增长和变化，网络可以平滑地扩充和升级，减少最大程度的减少对网络架构和现有设备的调整。

——可管理性:对网络实行集中监测、分权管理，并统一分配带宽资源。选用先进的网络管理平台，具有对设备、端口等的管理、流量统计分析，及可提供故障自动报警。

#### 8.5.1 网络体系架构

远程医疗信息系统网络按照分层设计原则，分为国家中心、省级中心、接入机构三部分。如图 3-10 所示：

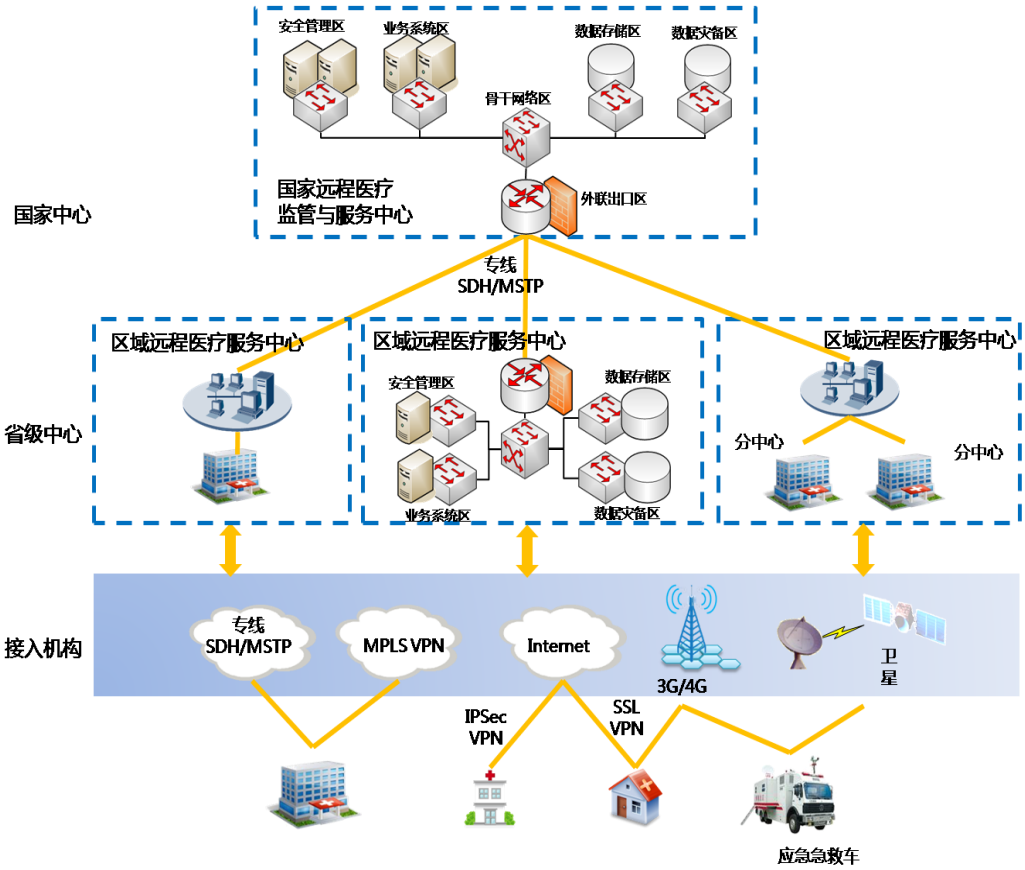


图3　远程医疗信息系统网络拓扑图

国家级远程医疗监管与资源服务中心为远程医疗系统网络的核心节点，对各级远程医疗系统建设和日常业务开展起规划指导和协调管理的作用，促进全国医疗资源的协调分配。数据中心内部按照模块化的设计原则，分为外联出口区，骨干网络区，业务系统区，安全管理区，数据存储区和数据灾备区。

省级中心连接二三级医院、乡镇医院、社区卫生服务中心、救护车的网络接入，协同各个接入单位的远程医疗的业务。实现本省的远程医疗基本功能和对远程医疗服务的监管与服务。实现与国家远程医疗监管与资源服务中心、省级卫生信息平台的互联互通。

接入机构为远程医疗信息系统的基本组成单位，通过专线，MPLS VPN，Internet，3G/4G，卫星等多种手段接入省级中心。

国家远程医疗监管与资源服务中心和区域远程医疗监管与资源服务中心主要负责远程医疗业务的协同与监管。各医院之间视频和数据业务流，建议不经过两级服务中心，由参与业务的医院通过互联网或者专网建立连接。

部署中，省级节点负责省级以及以下节点的接入、网管，国家节点负责国家到省级之间的网络链路状况管理，包括基本路由等功能。

网络平台中针对业务进行可识别性管理包括资源应用的监控，并提供图形化的管理界面。

### 8.5.2　远程接入

#### 8.5.2.1　接入单位设计

省级和市县级医疗机构：其特点为病人流量大、医院规模大、地理位置距离地市中心数据中心较近。采用专线方式和/或 MPLS-VPN 直接连入区域远程医疗监管与资源服务中心，实现业务系统的高速访问，

同时为保障业务的稳定开展，有条件的单位采用专线、MPLS-VPN 和 Internet VPN 等方式做为备用链路连入数据中心。建议采用两个不同运营商保证高可靠，当主要链路故障时，能够自动切换到备用链路，确保业务的 7*24 小时不中断。

乡镇社区医疗机构：如大型乡镇卫生院、偏远社区卫生服务中心等。其特点为病人流量不大、医院规模较小、地理位置距离数据中心较远。此类单位由于距离较远，所有单位直接连入数据中心将大大提高链路成本。根据实际链路带宽、可靠性、时延等实际需要，考虑使用专线、MPLS-VPN 或者 Internet VPN 方式接入数据中心。建议使用双链路保证可靠性。

应急急救车:应急急救车需要能够支持到各种地区，有些地区没有有线链路，需要采用 3G/4G 或者卫星的模式接入中心。

#### 8.5.2.2 接入链路设计

远程医疗信息系统由于覆盖的医疗卫生单位的种类很多，物理位置相对分散。这些医疗卫生单位由于地理位置的原因或者规模的要求，对于传输网络的要求都不相同。各单位可根据各自的特点，选择如下的接入链路：

专线: SDH 专线基于时分复用技术，网络时延小，稳定性高，提供丰富的检、纠错能力。对用户来说，SDH 在链路上相当于一个透明的物理通道，在这个透明的通道上，只要带宽允许，用户可以开展各种业务，如语音、数据、数字视频等，而业务的质量是用户可控的。另一方面，SDH 专线租用费用较高；点对点的连接，网络管理较复杂。建议国家中心和省级中心之间，以及二/三级医院与中心之间采用此种连接方式。

MPLS-VPN：运营商在专门建设的 IP 专网上构建企业用户的虚拟专网。相对于 SDH 专网，租用费用较低；部署和管理简单。由于物理链路由多企业共享，链路的服务质量由运营商控制。建议二/三级医院采用此方式与中心互联。

Internet VPN：Internet VPN 利用互联网线路，通过 VPN 技术将分支机构或单人连接到企业网络。在互联网上传输数据需要建立一个安全加密的数据传输隧道。安全加密的 VPN 技术有 IPSec VPN 和 SSL VPN 两种。通常采用 IPSec VPN 建立网络之间的连接，采用 SSL VPN 建立终端到网络之间的连接。Internet VPN 的优点在于接入方便，费用低。同时缺点也很明显，网络时延较大，网络质量不可控，语音视频业务体验差。建议没有专线资源的乡镇医院和社区服务中心，采用此种方式。若医院/社区服务中心有自己的局域网，建议采用 IPSec VPN 方式，反之采用 SSL VPN 方式。

3G/4G 链路：使用 3G/4G 接入，不受地理条件限制，尤其是山区等不适宜部署有线网络的场景。3G/4G 接入的劣势在于带宽小，资费较高。建议在没有有线接入点的社区服务中心，作为接入链路，或者在有线可靠性无法保证的区域使用 3G/4G 链路作为备份链路。应急急救车也可以在没有有线网络的场所选用此种方式。

卫星专线：卫星专线业务利用由卫星地面站和通信卫星组成的卫星通信系统向用户提供的点对点传输通道、通信专线出租业务。卫星专线最大的优点在于不受地理条件和地面线路资源限制，结构简单，无需经过复杂的地面路由。卫星专线缺点在于延时大，租用费用高。建议应急急救车采用此种方式。

### 8.5.3 网络可靠

#### 8.5.3.1 设备可靠性

——网络设备交换引擎、接口、风扇、电源等冗余配置；

——核心路由器/交换机支持数据转发和控制分离，保证在控制层面出现故障时，数据转发仍然正常执行，从而保护网络上关键业务不受影响；

——核心路由器支持不间断路由。保证在控制层面出现故障而进行主备倒换的时候，与此路由器相

邻的路由器不会感知这次故障，从而避免路由的重新计算，导致网络震荡；

——核心路由器/交换机支持版本升级不中断业务。设备运行过程中经常需要升级软件版本，升级版本过程，设备支持业务转发不中断。

#### 8.5.3.2 设备间可靠性

——路由器支持 VRRP。VRRP（虚拟路由器冗余协议）可以把一个虚拟路由器的责任动态分配到局域网上的一组路由器中的一台。在某台路由器故障时，所辖的网络设备正常工作，不感知到此次故障；

——交换机支持虚拟化，减少配置维护复杂度，增加可靠性。

#### 8.5.3.3 链路可靠性

——核心路由器/交换机支持故障快速感知。故障快速感知技术是故障快速切换保护的基础，只有实现故障的快速发现，才能实现故障的快速切换保护。建议网络设备能够在系统之间的任何类型通道上进行故障检测，这些通道包括直接的物理链路，虚电路，隧道，MPLS LSP，多跳路由通道，以及非直接的通道。检测周期可达到 10ms；

——核心路由器支持快速重路由。即支持预先设定主备路径，建立绑定关系；通过设备故障快速感知发现故障后，直接切换到备份路径，优先于 OSPF 等 IGP 的收敛速度。要求收敛速度达到端到端 100MS。

### 8.5.4 网络管理

#### 8.5.4.1 设备管理

——支持统一管理华为、H3C、CISCO、中兴等主流网络厂商的网络设备，以及 IBM、HP、SUN 等主流 IT 厂商的 IT 设备，同时应该提供灵活的自定义能力。对于没有预置的设备，用户可以进行自定义，经过自定义后可以同预置设备一样进行管理；

——支持对实现标准 MIB（RFC1213-MIB，Entity-MIB，SNMPv2-MIB，IF-MIB）的设备的管理。

#### 8.5.4.2 拓扑管理

——支持以拓扑图的方式直观的显示了网元及其之间链路连接的关系和状态。用户可以通过拓扑管理全局把握全网设备的层次结构和运行状态；

——支持物理拓扑和 IP 拓扑两种拓扑展示方式。

#### 8.5.4.3 告警管理

支持对网络中的异常运行情况进行实时监视，通过告警监控板、实时告警浏览、历史告警浏览、事件列表查看等功能对网络故障进行监控。用户可以根据需要设定告警的远程通知规则、告警屏蔽规则和告警的声音。

——提供多个界面对不同的告警数据进行浏览；

——通过图形板快速显示当前活动告警的数目；

——提供对当前活动告警的浏览。支持按照用户设定条件监视符合条件的告警上报；

——支持按照用户设定条件搜索告警；

——提供对不活动、已经归档成历史的告警进行浏览；

——提供对设备上报的事件进行浏览；

——提供对网管屏蔽的告警进行浏览。

#### 8.5.4.4 配置文件管理

支持对设备的配置信息进行管理，提供对设备配置文件的导入、备份、恢复、比较、基线化管理。当网络出现问题时，可以根据之前备份的网络可运行时的配置文件与当前设备正在运行的配置进行比较，快速定位并恢复当前出现的故障。

——支持备份任务：按日、周、月为周期，按设定时间对任务所包含设备的运行配置文件进行备份。支持设置设备配置变更告警触发备份配置文件。备份任务可以按照定制的时间进行定时备份，也可以对备份任务进行立即备份操作；

——配置文件基线化：对指定设备的运行配置进行备份，将选定的设备的配置文件恢复成设备的运行配置，对选定的配置文件进行基线化，同时能够方便的查看设备上面的运行配置；

——配置文件比较：对于已经备份到本地的配置文件，可以进行查看、比较文件差异和删除的操作。文件比较功能当前提供了已经备份到网管服务器的配置文件之间的比较。

### 8.5.5 音视频数据网络质量及 QoS 需求

——网络时延小于 50ms

——Jitter 尽可能低，不大于 20ms 最佳

——丢包不大于 5%

## 8.6 视讯系统

### 8.6.1 业务管理系统技术要求

——统一通讯管理系统实现设备管理，注册认证，会议管理，会议控制，报表统计等功能。支持 B/S 架构，需采用独立的硬件服务器，不能采用 MCU 的内置 web。

——采用独立的 GK 服务器或内置于业务管理平台的 GK 服务器，用于设备的注册、鉴权。GK 服务器支持不低于 1000 个结点的注册，GK 服务器最大可支持到 6000 个结点或以上注册。

——需支持 IPv4 和 IPv6 双协议栈。最多可扩容支持不少于 128 台 MCU 设备的管理，不少于 10000 个会场的管理。

——支持按组织结构管理用户权限，用户权限可以配置。提供系统管理员、会议管理员和普通用户三个权限组。

——支持分级分权管理，系统权限和资源按照企业组织结构树状管理，同一台 MCU 或者会场能够分配给多个组织使用。

——支持设备（MCU 和会场）按组织结构方式管理。

——支持远程添加并管理 MCU 和终端设备，不仅能够查看终端或者 MCU 的品牌型号、GK 注册状态、SIP 注册状态、MAC 地址，终端/MCU 的视频能力，软件版本号等信息，还能够实时远程修改设备配置，例如远程开启、关闭 GK 注册，远程修改 H.323ID、E.164 号码、DNS 服务器地址等。

——支持管理主流视讯终端设备（例如：思科/宝利通/华为），不仅能够查看终端的品牌型号、GK 注册状态、SIP 注册状态、MAC 地址，终端的视频能力，软件版本号等信息，还能够实时远程修改设备配置，例如远程开启、关闭 GK 注册，远程修改 H.323ID、E.164 号码、DNS 服务器地址等

——支持设备自动发现功能，设备（MCU 和终端）加入系统后自动被管理平台识别，发现设备后可对设备进行信息查看和配置，并且支持对被管理设备的配置备份和远程恢复。

——支持系统告警管理，实现远程查看被管理设备（终端和 MCU 等）告警信息，并且针对告警类型进行分类，快速获取被管理设备的运行状态。

——支持对被管理设备的日志进行远程查看。

——支持对录播服务器设备进行远程管理和远程控制。

### 8.6.2 MCU 技术要求

#### 8.6.2.1 国家平台 MCU 技术要求

——要求采用嵌入式操作系统，非 Windows、Linux 系统；不能采用 PC 架构，不得为工控机架构(无鼠标键盘和 VGA 接口。设备要求为插卡式设计，能够通过增加板卡实现系统容量的平滑升级；设备每块板卡上具备至少 2 路 1000Mbps RJ-45 电口和 2 路光纤接口，且能够同时支持 IPV4 和 IPV6。

——支持每个参会终端均以不同的协议（H.323/SIP）、不同的带宽（64K-8Mbps）、不同的音视频编码(H.263/H.264 等，G.722/G.711/AAC-LD 等)、不同的清晰度（CIF/4CIF/720P 30fps、60fps/1080P 30fps、60fps）同时加入到一个会议中，且同时能够支持多组会议，会议组数不受混网、混速数量的限制。

——呼叫带宽支持 64Kbps-8Mbps，系统容量最大支持不少于 84 个 1080P60fps 或者 168 个 1080P 30fps/720P60fps 或者 336 路 720P 30fps 或者 672 路标清（CIF/4CIF）会场同时接入，除此之外设备还能够同时支持 168 路纯 IP 语音会场呼入。通过人工指定可以将 MCU 的端口资源根据视频清晰度任意分配，达到资源利用最大化，MCU 端口资源分配不用重启 MCU 设备。

——支持 ITU-T H.261、H.263、H.263+、H.264 Basic Profile、H.264 High Profile、H.264 SVC 视频协议。支持 1080P60 帧、1080P30 帧、720P60 帧、720P30 帧，并向下兼容 4CIF、CIF 图像格式。

——支持 ITU-T G.711a、G.711u、G.722、G.728、G.722.1C、G.729、iLBC 音频协议,支持具备 20KHZ 频响的宽频语音编码 G.719、AAC_LD、HWA_LD 音频协议, 支持一个会场同时传输两路音频区分左右声道，实现立体声效果。

——支持 2/3/4/5/6/7/8/9/10/13/16/20/24 等多画面类型，具有多画面模式切换，支持 VIP（N+1）格式的多画面（例如 5+1、7+1 多画面显示）。支持自定义参会会场在多画面中的显示位置。支持每端口多画面，支持参会的终端设备通过 FECC 方向键或者遥控器按键选择自己会场独特的多画面组合方式，并且其他会场清晰度、观看多画面方式均不受影响。支持将辅流加入多画面中，以便让不支持 H.239 的终端设备收到辅流信息。

——支持主控板和媒体板热备份，且主控板在倒换过程中不影响正在召开的会议，支持双电源冗余备份。设备支持 H.235(AES256)、SRTP、TLS、HTTPS、SSH、SNMP V3 等媒体、信令、管理加密，提供身份验证与加密通讯的安全通道，防止用户被仿冒，保护会议信息在传送过程中不被截获翻译，全面保证会议信息安全。

——支持标准 H.239 双流和 BFCP 双流，支持静态双流和动态双流，辅流带宽可以按需要手工设置，辅流最大支持 1080P 60fps 图像格式。支持辅流适配功能，在一个高清、标清混合的会议中，能够实现不同视频解码能力的终端接收到不同清晰度的辅流信息，保证不会因为某个参会会场辅流接收能力较低而影响其他会场。

——支持音视频 IVR 功能，与会终端可以通过呼叫 IVR 接入号或者直接呼叫 MCU 的 IP 地址，并根据系统提供的音视频 IVR 引导，方便的实现会议的创建或者加入到已经召开的会议中。

——支持多通道级联技术，下级 MCU 多个会场能够通过多个独立的视频通道传到上级 MCU。

——MCU 设备具备较强的抗丢包能力，在 10% 丢包下，语音连续清晰，视频清晰流畅，基本感觉不到丢包影响；在 20% 丢包下，语音较清晰连续，视频偶有卡顿。要求具有权威检测机构的证明报告。

#### 8.6.2.2 区域平台 MCU 技术要求

——要求采用嵌入式操作系统，非 Windows、Linux 系统；不能采用 PC 架构，不得为工控机架构(无鼠标键盘和 VGA 接口，卖方要详细描述 MCU 体系结构。

——要求采用插框式结构，可以通过增加插板的方式平滑增加接入容量，方便系统扩容，系统业务板卡数大于等于 8 块，确保后续扩容能力；要求媒体处理单板为通用处理板，每个单板可实现视频、音频、双流和接入等媒体处理功能；要求采用无源背板技术，所有单板都支持带电热插拔，自动正常启动。

——支持多分屏和速率适配模式下的 512 路带宽 4Mbps 的 1080P 会场接入容量,支持接入远程呈现会场路数不少于 170 路。支持以插板扩容方式接入大容量语音会场，最大支持 4900 路语音会场，其中语音会场可以采用 H323、SIP 协议 VOIP 接入。

——支持 ITU-T H.261、H.263、H.264 视频协议。支持 1080P60 帧、1080P30 帧、720P60 帧、720P30 帧，并向下兼容 4CIF、CIF 图像格式。

——支持 ITU-T G.711、G.722、G.728、G.729 音频协议,支持 22Khz 频响的宽频语音（AAC-LD、AAL-LC），支持一个会场同时传输两路音频区分左右声道，实现立体声效果。

——要求采用全新的硬件平台支持 1080p、720p，而非仅靠升级软件实现，能够支持 1080P30fps 和 720P 60fps 多画面,并采用对称视频编解码而非画面组合方式，平台具有强大的兼容性和可扩展能力，支持辅流加入多画面显示。

——支持高清、标清终端混速混协议召开会议，允许不同编解码格式，包括 1080P、720P、4CIF、CIF 等终端参加同一个会议，支持多个编解码格式的会议同时召开。单个会议能支持不少于 5 种速率协议适配能力。

——支持业务接口板（含主控板和业务板）1＋1 的热备份，支持 IP 网口的 1＋1 的热备份，网口业务切换时不影响正在召开的会议，支持电源模块的 1+1 备份。

——支持会议主席对会场摄像机远程控制功能,支持会议管理员通过会议管理平台对任意入会会场的摄像机远程进行放大缩小和上下左右移动。

——支持国际标准的信令加密和媒体流加密，全方位保护会议安全。

——支持 H.239 双流和 SIP 双流，支持静态双流和动态双流，各终端可以相互发送双流，辅流带宽可以按需要手工设置，可以达到主流辅流都为 1080P 30fps 高清活动图像效果。

——MCU 支持 8%的丢包情况，声音连续，视频有少量马塞克，可马上恢复。

### 8.6.3 高清会议终端技术要求

——要求采用嵌入式操作系统，非 Windows、Linux 系统；非 PC 架构，非工控机架构。

——至少支持两路 DVI-I 输入/输出接口，并可实现即插即用输入；支持 HD-SDI 输入/输出接口，高清终端和摄像机或矩阵之间可以达到 100 米的传输距离信号无明显衰减,方便大型会议室摄像机远距离布置；支持通过一根 HDMI 线缆连接电视机，同时输出视频和声音，方便连线和维护。；具有标准的卡农头麦克风接口；支持不少于两路的摄像机控制接口。

——终端应具有 USB 接口，可以扩展接入 USB 接口 3G 数据卡，并支持通过 3G 网络进行无线远程视频通讯。

——视频支持 H.263、H.264 图像编码协议，图像格式支持 1080P30 帧、720 P 60 帧、720 P 30 帧、4CIF， CIF。

——音频支持 G.711、G.722、G.728、G.729 系列，并且支持 AAC-LD（22KHz 频响）宽频音频标准，支持双声道立体声功能。

——支持标准 H.239 协议和 BFCP 的双流收发,辅流 PC 桌面数据输入输出都能达到 1280*1024 的分辨率；支持 2 路高清活动图像，可支持 2 路 720p30fps 双流收发。支持信令和媒体流加密算法，保证会议安全。

——支持网络抗丢包能力，在 IP 网络达到 8%丢包时，声音连续，视频无明显马赛克。支持网络诊断功能。
——支持在两个显示设备分别显示远端（或本端）主流和辅流；支持在一个显示设备以画中画、二分屏、三分屏等多种模式同时显示 2 路或 3 路图像。
——支持 IP 网络升速、降速完全自适应，即根据 IP 网络带宽的变化，自动调整会议中视音频带宽，保证图像语音质量良好。
——终端支持 SNMP 协议，可以通过网管系统远程管理，通过网管统一修改配置终端参数。
——终端支持红外遥控操作，可以通过遥控器直接对终端控制；在终端隐藏在机房或电视机后面时，遥控器也可以通过终端配套的摄像机遥控终端
——全中文图形化界面，支持遥控器中文输入，应具有基本的维护检测功能，本端音频自环、视频自环、远端环回、事件日志、远端升级维护等功能。
——终端支持静态 NAT、H.460 等公私网穿越协议，支持固定信令和视音频端口进行防火墙穿越。
——终端支持休眠功能，空闲到启用休眠功能的时间可配置，呼叫、遥控器/web 操作、来电等支持自动唤醒。
——支持 LDAP 地址本，支持 LDAP 访问认证和加密。
——要求具备电信设备进网许可证，支持 CCC 认证。

### 8.6.4 高清摄像机技术要求

——支持 12 倍光学变焦，4 倍数字变焦，支持 1080P 50/60fps、1080i 50/60、1080p 25/30、720P50/60fps 视频输出。
——支持 200 万像素 1/3 英寸 CMOS 成像芯片，最大水平视角 72°，最大垂直视角 44.5°。
——支持 3G-SDI 视频输出接口，摄像机和终端可以达到 100 米以上，1080P60 图像的无损传输。
——支持摄像机倒装，便于摄像机倒装在天花板上。
——支持通过按键设置摄像机视频输出格式，不需要重启摄像机。支持 LCD 显示功能，可以实时显示当前视频输出格式和故障码，便于维护人员诊断和维护。
——支持低照度下的背光补偿，支持通过终端遥控器或 WEB 界面对镜头视频格式、曝光指数、白平衡、对比度和降噪等参数进行远程调整。支持标准、鲜艳、柔和三种图像模式的选择。

### 8.6.5 数字麦克风技术要求

——数字麦克风，支持 360 度全向拾音，最大拾音距离达到 6 米。
——通过 PoE 口供电，不需要额外电源。
——支持自适应回声抵消，自动增益控制，自动噪声摄制。
——采样率不小于 48KHZ。
——支持通过麦克风的触摸面板进行闭音和开音操作。

### 8.6.6 网络录播系统技术要求

——网络录播服务器支持 B/S 架构，可以通过 WEB 轻松访问，实现点播、直播功能；
——系统支持 IPV4 和 IPV6 双协议栈，支持 IPv4 单独组网、IPv6 单独组网或者 IPv4/IPv6 混合组网。
——网络录播系统最大支持同时 30 组 1080P30 会议录制；
——支持同时录制一路高清和一路标清图象，各分支节点根据网络状态选择高清或者标清点播观看；
——系统支持会议的双流录制，辅流录制支持 1920*1080 高清录制；

——支持单点、点对点和多点会议的录制；
——支持对录制会议的过程进行控制，包括：录制、暂停、停止、选择录制源。
——支持 PC、IOS、Android 手机、PAD 平台直播和点播录播服务器视频；
——支持浏览器免插件直播和点播；
——支持在 PC 浏览器上预览录播图片和文字索引；
——支持直播、点播过程中主辅流和声音同步播放；
——PC 浏览器直播、点播时，支持对画面布局进行切换；
——浏览器进行点播时，用户可以对点播内容进行暂停（播放）、定位、停止、全屏（取消全屏）、音量调节等操作。

## 8.7 联络中心

### 8.7.1 联络中心总体要求

联络中心应提供多媒体联络中心，支持语音、视频、传真、email、短信、在线客服、社交媒体的多渠道服务模式，实现集被动服务、主动服务、主动营销为一体的多元化运营平台。

### 8.7.2 排队机设备要求

#### 8.7.2.1 设备基本配置要求

——支持多种信令方式，必须支持包括七号信令（SS7）、中国一号信令（No.1）、ISDN PRI 信令、SIP 等等各种宽窄带信令，各信令由一种 E1 硬件板卡上实现，信令变更时无须更换硬件，只需软件设置即可；
——交换机系统内核必须同时支持电路交换(TDM)和分组(IP)交换，分组交换应支持 SIP 协议；
——接入设备独立运行时支持的最大中继数量应不小于 10 个 E1，单个网关设备支持的呼叫并发数量应不小于 300 个；支持的数字中继板（连接 PSTN）数及每块板支持的路数必须不小于 90 路；
——系统应支持外呼功能，并提供对应答信号自动检测功能（如无人接听、占线、FAX、应答机等），以支持预测式外呼应用；
——排队机支持内置传真功能,支持宽窄带的传真发送和接收,可接收或发送单页传真和多页传真。
——提供自动应答/自动溢出、超时应答、重定向、主叫信息转发等功能；
——排队机应能提供 TSAPI 或者 SCAI 等接口，能实现与第三方 CTI 平台软件对接；
——排队机系统内部机架支持通用槽位，且所有功能电路板支持热插拔；
——提供中文图形化界面的网络管理软件；
——应支持密码的设置。

#### 8.7.2.2 设备可靠性要求

——排队机为了保证较高的安全性和可靠性，应使用嵌入式实时操作系统，增加排队机的信令处理能力和抗病毒的高安全性和稳定性；
——排队机应具有很好的容错性及高可靠性，主要模块冗余配置并能够实现热切换；
——排队机系统支持内置的排队功能，提供硬排队路由功能。
——交换机系统需提供内置 N+1 冗余整流电源模块，电源模块支持热插拔，各机框分电源均需冗余备份。
——系统应提供主控单元热备份，在单板故障时自动倒换到备份上，不中断业务。
——交换机系统中不同硬件设备的连接类，控制类单板需要主备。包括交换机之间、交换机和 CTI 平台之间、交换机和其他服务器之间。

### 8.7.3 呼叫中心系统平台功能要求

#### 8.7.3.1 计算机电话集成（CTI）要求

——支持基于多种技能的路由，每个技能组应支持不小于 100 种技能，每个技能支持不小于 50 种不同的技能级别；
——CTI 产品应支持通过交换机提供的 CTI Link 连接 PBX；
——支持多媒体统一排队功能，支持用户通过电话、Email、传真、Web、视频等多媒体呼叫的无缝统一路由功能；
——CTI 平台可支持 Unix、Linux 和 Windows 平台，支持主备组网方案；
——支持记录操作人员的上下班情况、记录操作人员离席情况、记录每个座席的接答情况、记录各个分组及分机的情况（全忙、等候、通话等）。
——支持人工座席与自动流程之间呼叫与数据的同步、任意无限制转移。
——支持向 ACD/PBX 发送与呼叫相关的指导性控制指令，完成呼叫定向、重定向、排队、与呼叫相关的资源管理等功能。
——支持呼叫转移时，转移方挂起等待，直到转移的呼叫由目标方挂断后并返回转移方继续处理。
——平台支持虚拟化技术，能将媒体资源、中继资源、IVR 资源、录音资源等进行虚拟化分割，实现一个平台虚拟出多个完全独立的虚拟呼叫中心平台。
——支持无 ACD/PBX 设备环境下的仿真开发，即提供模拟开发环境，并实现模拟开发环境开发的业务可以用于现网业务实现。
——CTI 连接必须提供冗余热备份，保证系统不因单一 CTI 接口的故障造成运行中断。
——系统开放 TSAPI 接口和 SCAI 接口，支持与第三方系统 CTI 系统对接。
——CTI 系统必须具有很强的业务融合能力，很好的支持二次开发。系统应配置通用的开发接口和丰富的开发工具。能够对外提供包括 WebService 和 ActiveX 等开发接口。
——CTI 平台必须具备各功能组件统一的集中管理，集中配置能力。对配置的重要信息具备用户口令认证及权限分配机制。
——CTI 平台必须具备告警功能，当出现能引起操作上的扰动或需要人工干预或性能超过预定操作门限时，产生告警指示。

#### 8.7.3.2 网络呼叫中心功能要求

网络呼叫中心应提供多个中心统一管理功能，实现呼叫统一分配、资源完全共享、全网负载均衡。支持网络路由、网络排队、网络呼叫转移、网络资源管理、网络监控、网络质检等功能。

#### 8.7.3.3 智能路由和排队处理能力要求

CTI系统平台应能够根据：主叫号码，被叫号码，呼叫位置，按键信息，客户数据库，坐席状态，坐席技能，呼叫时间，呼叫成本等信息制定路由规则。

#### 8.7.3.4 分层服务功能要求

网络呼叫中心应能够根据不同客户群的特点，提供差异化服务，能为 VIP 客户提供更加优质的服务，支持黑名单功能等。

#### 8.7.3.5 座席呼叫控制功能

座席应能够向平台系统注册（通过工号和密码进行登录），统计每天由登录时间作为考勤，客户来电后，系统通过智能路由功能自动将来电转接至已登录且最合适的座席，系统应能够按负荷均衡等多种

策略进行路由。

### 8.7.4 自动语音(IVR)系统功能要求

——IVR 系统应可以根据不同的拨入号码启动不同的业务逻辑流程，应能够支持清晰、准确的语音导航、录音、放音、收号的功能功能；
——IVR 系统应采用硬件 DSP 编解码方式提供 IVR 媒体资源；
——单台 IVR 服务器能够支持不小于 800 路并发呼叫；
——IVR 系统应支持语音流程控制；
——IVR 系统应支持连续拨号，支持语音打断功能；
——IVR 系统应支持灵活的脚本流程控制语言，支持图形化的全中文自动业务流程开发工具，支持通过拖拽方式迅速、灵活地生成新的自动业务流程，并能进行仿真测试，实时在线业务加载。
——IVR 系统应支持多种开发接口；
——多台 IVR 服务器应采用负荷分担方式工作，且不能影响整体 IVR 端口的 LICENSE 数量，系统应支持自动分配 IVR 的 LICENSE 端口；
——IVR 系统应具备完整的图形化实时监控和管理工具，支持多点集中监控、统一管理和实时在线业务加载；
——IVR 系统用户接入有提示音应不大于 1 秒，收号准确率应不小于 99.96%；
——支持文本语音转换(TTS)与自动语音识别（ASR），支持 NUANCE 与科大讯飞等世界著名厂商的语言识别引擎；
——支持自动传真（FAX）功能、定时收发传真、批量收发传真、文本格式(*.txt)转换为*.tif 传真文件格式。支持 T.30 和 T.38 等宽窄带传真协议；
——IVR 系统应支持业务转移功能；
——IVR 系统应支持多个呼入号码对应不同的欢迎语来满足不同客户服务中心的需要；
——IVR 系统应支持根据客户级别的高低进行分级处理；
——IVR 系统应支持多种操作系统，如 Windows、Linux 和 Unix 等。
——IVR 系统应支持放音功能，支持播放常用提示音、本地文件、整数、浮点数、字符串、价格、日期、时间、汉字字符串合成音、汉字文本文件合成音等。

### 8.7.5 外呼管理系统

——支持多种外呼模式，包括预览式外拨、预测外拨和预占用外拨方式。
——支持预测式外呼,并提供智能呼入呼出混合模式,自动外拨数量可根据呼入压力自动动态调整，座席完成呼入呼出工作状态的切换无需进行二次登录，能充分整合呼入及呼出业务，系统根据座席忙闲、业务逻辑提供多种调度机制，实现话务均衡，并实现统一的呼入呼出报表。
——支持多媒体外呼，实现自动语音和人工外拨渠道。
——支持处理多个呼出任务,每个呼出任务可以规定该任务的启动时间、每次同时发起的呼叫数目、本任务发起的呼叫所需的服务需求、呼出失败的处理方式。
——支持对不成功外拨的灵活处理，支持通过呼叫过程侦测所检测到不同外拨结果，分别设置不同的处理方式。
——支持全中文的管理、监控界面，随时监控外拨系统运行状态，和外拨列表处理情况。
——支持完善的登记待呼出记录的功能以及完善的呼出失败记录管理的功能,支持同时多个呼出任务的处理。
——支持完善的外拨报表统计，支持报表定制功能。
——支持数据库接口和 WEBSERVICE 接口，供第三方业务管理系统集成。

### 8.7.6 质检功能

——支持基于 WEB 方式进行质检管理，并可在线对座席进行监视、监听、监察、插入、强制签出、拦截、强制示忙/示闲/释放、全屏质检等质检操作；
——支持质检考评系统，包括质检关系管理、考评项管理功能。支持事后质检和实时质检。并支持对质量分析从质检结果、考评项结果、质检量、特殊流水量四个方面进行多维度的统计比较分析；
——支持座席状态察看；
——支持座席监听；
——支持座席录音管理；
——支持实现监视、监听/监察、插入、强制签出、拦截、强制示忙/示闲/释放、全屏质检等质检操作；
——支持通过电脑监控其它受理座席的详细受理情况（电话排队情况、座席状态（示忙、通话、离席）、当日受理情况）等；
——支持随时看到各受理座席 PC 的实时屏幕图像功能；
——支持大屏幕监控；

### 8.7.7 监控管理系统

——支持权限控制方式，具有不同权限的用户只能进入相应的监控界面，查看相关设备运行信息。

### 8.7.8 录音录屏系统

——支持录屏功能,录制指定业务代表的屏幕操作情况。支持同时录制业务代表与客户的通话内容。
——支持录制的内容通过 FTP 方式上传到 FTP 文件服务器，或通过目录共享方式上传到共享磁盘；
——支持多种语音压缩比率，充分利用存储空间，降低系统成本；
——支持多种录音方式，包括强制录音、质检员指定座席录音和座席自录音等方式，坐席通话支持全程录音，可随时调听；
——支持实现录音按日期、时间、主叫号码、被叫号码、坐席工号等多种搜索条件进行查询；
——录音系统应提供开放的 API，供第三方系统来查找录音文件；
——录音系统能够满足连续 7×24 小时不间断工作的要求，有很高的安全可靠性；
——支持实时监控功能，满足管理人员实时监控要求；
——支持多种存储介质方案，录音可保存至 SAN 或 NAS 外部存储系统、适应大容量录音应用；
——支持录音文件的远程播放功能；
——支持灵活录屏方式，包括手工录屏和自动录屏。

### 8.7.9 传真系统

——系统应支持通过语音导航形式实现传真的自动收发功能；
——传真模块应支持设置禁发传真的号码；
——支持多种传真应用，如传真回复、传真接收、在线发送传真、离线发送等，且允许不同的传真处理应用同时执行；
——支持传真收发历史记录；
——支持 10 路以上的并发传真处理；
——支持与电子邮件服务器直接交互；
——支持结合 IVR 自动语音系统，提供多种传真业务服务；

#### 8.7.10 在线客服功能要求

——支持通过文字方式和多媒体等多种方式向用户提供服务信息；
——系支持主动与用户进行智能交互，为用户提供更有针对性的服务或信息；
——支持通过点击通话和座席员进行语音交流；
——支持整合业务知识库，支持提供各种业务知识、查询等在线查询服务；
——支持服务质量评价；
——支持社交媒体的功能，包括社交媒体的接入、信息发布和管理、支持关键字搜索功能、社交媒体信息标记、座席处理和回复审核功能。

#### 8.7.11 报表

——支持对多种数据库的支持，包括 SQL SERVER、Oracle 等大中型数据库，统计内容设定应采用开放式结构，支持基于 SQL 等常用语句的统计内容设定；
——支持基于 WEB 方式访问；
——支持多种媒体的统一报表，包括语音、文本、传真、邮件等多种媒体；
——支持报表格式可灵活定制；
——支持周期报表，可生成一次、按天生成、按周生成和按月生成；
——支持实时报表统计；
——支持直接对统计报表的打印，支持以 Excel 文件格式保存统计报表文件；支持对 Excel 文件模版的修改。
——支持产生统计信息图表；
——支持提供基本的通话清单。话单包括呼叫标识、主叫号码、被叫号码、等待开始时间、等待结束时间、应答开始时间、应答结束时间、通话开始时间、通话结束时间、业务类型号、等待原因、释放原因等。
——支持提供中继统计报表、话务量报表、IVR 报表、技能报表和话务员报表等。
——呼叫记录的数据应至少保存 3 个月，可根据用户需求确定保存时长，并确定所需存储配置。

### 8.8 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。目前对于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1 医院灾备系统 RTO/RPO 等级要求**

| 灾难恢复等级 | 恢复时间（RTO） | 可接受的数据丢失（RPO） | 医院规模 | | |
|---|---|---|---|---|---|
| | | | 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。

### 8.9 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

遵循《基于电子病历的医院信息平台技术规范》9.1。

### 9.2 物理安全

遵循《基于电子病历的医院信息平台技术规范》9.3.1。

### 9.3 网络安全

#### 9.3.1 概览

对远程医疗信息系统进行各个层面的安全威胁分析和需求分析，如下表所示：

| 安全威胁/需求 | 各场景中安全威胁/需求的位置/对象 | 解决方案 | 相关产品/技术 |
|---|---|---|---|
| 网络攻击及互访控制 | 数据中心出口边界<br>接入单位出口边界 | 边界隔离 | 防火墙/安全网关 |
| DDoS 攻击 | 各外部出口：带宽<br>数据中心：业务服务器 | 流量清洗 | AntiDDoS<br>防火墙/安全网关 |
| 基于漏洞、后门的应用层入侵攻击 | 接入单位：办公终端<br>数据中心：业务服务器 | 入侵防御 | IPS/IDS |

| | | | |
|---|---|---|---|
| 病毒传播 | 数据中心：业务服务器 | Anti-Virus | Anti-Virus 网关 |
| 明文接入被窃听、篡改 | Internet VPN | 加密传输 | IPSec VPN |

### 9.3.2 基础网络安全

遵循《基于电子病历的医院信息平台技术规范》9.3.2。

### 9.3.3 安全区域边界安全

——Internet 出口部署防火墙

- 进行 NAT 转换：实现内部服务器对外映射公网地址；实现内部用户上网时进行源地址 NAT 转换；
- 进行访问控制：部分对外提供业务的服务器可以允许外部用户访问；其他业务仅允许由内部发起向外部的访问，且可对业务协议及类型进行控制；
- 可以做 VPN 网关：可作为互联时的 IPSec VPN 网关。

——数据中心各区域出口部署防火墙

- 进行访问控制：对各个不同安全等级的区域之间互访进行控制，例如，医疗系统和管理区的隔离；各区域到数据中心区域的访问策略等。

——防火墙需要支持下列安全特性

- 基于安全区域的隔离：防火墙的安全隔离是基于安全区域，这样的设计模型为用户在实际使用防火墙的时候提供了十分良好的管理模型。防火墙提供了基于安全区域的隔离模型，每个安全区域可以按照网络的实际组网加入任意的接口,因此防火墙的安全管理模型是不会受到网络拓扑的影响。
- 可管理的安全区域：防火墙需要提供四个安全区域：trust、untrust、DMZ、local，在提供三个最常用的安全逻辑区域的基础上还新增加了本地逻辑安全区域,本地安全区域可以定义到防火墙本身的报文，保证了防火墙本身的安全防护。例如，通过对本地安全区域的报文控制，可以很容易的防止不安全区域对防火墙本身的 Telnet、ftp 等访问。
- 防火墙还提需供自定义安全区域，可以最大定义 16 个安全区域，每个安全区域都可以加入独立的接口。
- 基于安全区域的策略控制:防火墙支持根据不同的安全区域之间的访问设计不同的安全策略组（ACL 访问控制列表），每条安全策略组支持若干个独立的规则。这样的规则体系使得防火墙的策略十分容易管理，方便用户对各种逻辑安全区域的独立管理。
- 基于安全区域的策略控制模型，可以清晰的分别定义从 trust 到 untrust、从 DMZ 到 untrust 之间的各种访问，这样的策略控制模型使得防火墙的网络隔离功能具有很好的管理能力。

## 9.4 服务端系统安全

### 9.4.1 入侵防范

随着网络攻击技术的不断提高和网络安全漏洞的不断发现,防火墙无法发现隐藏在允许通过的流量中的应用层攻击，为解决这个问题可以根据预先设定的安全策略，通过 IPS 引擎感知并检测数据流量，逐个报文进行深度检测（协议分析跟踪、特征匹配、流量统计分析、事件关联分析等），如果一旦发现隐藏于其中的入侵攻击，可以根据该攻击的威胁级别立即采取抵御措施。

抵御措施按照处理力度可以分为：向管理中心告警；丢弃该报文；切断此次应用会话；切断此次TCP 连接；对滥用报文进行限流以保护网络带宽资源等。

对于数据中心的内部信息系统，需要部署入侵防御设备如IPS/IDS进行入侵检测或入侵防御，如防御下列安全

——虚拟补丁：防御漏洞利用攻击，使 IT 系统不再依赖软件补丁，提升服务器和终端的安全性，减少维护工作及非在线时间。

——客户端防护

- 提供浏览器及其插件（JS、ActiveX 等）的安全防护。
- 提供对 Word、PDF、Flash、AVI 等文件的防护。
- 提供对操作系统漏洞的防护。
- 支持间谍/广告软件的检测。
- 提供对偷渡式下载的防护。
- 提供对欺骗类应用软件的防护。

——Web 应用防护

- 保护 Web 应用服务，包括 Web2.0 及后台数据库。
- 提供对 SQL 注入攻击、跨站脚本等的重点防护。

——恶意软件控制

- 提供抵御木马后门、广告软件、恶意程序等恶意软件的能力。

——应用识别

- 支持基于知识库对应用协议进行识别。
- 支持对 850 种以上应用协议的识别。
- 支持对 P2P/IM/网络游戏/炒股软件/语音应用/在线视频/流媒体/Webmail/移动终端应用/远程登录等应用的识别。
- 知识库支持升级，以保证最新的最新应用识别能力。

——应用控制

- 支持按协议进行流量限制、连接数限制，有效实现游戏、股票、P2P 流量、IM 流量、VoIP 流量控制。
- 支持自定义应用协议集合，并对该应用协议集进行控制。
- 支持基于时间段、IP 地址段的应用控制策略。

——URL 过滤

- 支持对用户的 URL 请求进行访问控制，允许或禁止用户访问某些网络资源，达到精确管理上网行为的目的。

——流量型攻击防御

- 支持流量模型自学习。
- 支持对如下流量型攻击的防御功能：
  - ✓ TCP 泛洪攻击
  - ✓ TCP 连接耗尽
  - ✓ UDP 泛洪攻击
  - ✓ HTTP 泛洪攻击
  - ✓ HTTPS 泛洪攻击
  - ✓ DNS 泛洪攻击

- ✓ SIP 泛洪攻击
- ✓ ICMP 泛洪攻击

——报文型攻击防御

- 支持对扫描类报文型攻击的防御功能：包括 IP 地址扫描和端口扫描。
- 支持对畸形报文类报文型攻击的防御功能：包括 Teardrop、Ping of Death、WinNuke 等多种畸形报文类攻击。
- 支持对特殊报文类报文型攻击的防御功能：包括超大 ICMP 报文、ICMP 不可达报文、ICMP 重定向报文的控制、Tracert 攻击等多种特殊报文类攻击。

### 9.4.2 Anti-DDoS

分布式拒绝服务（DDoS）攻击是 Internet 上最常见的攻击之一。这些攻击通过向目标发送大量恶意请求，导致计算机服务器和网络设备的性能降低、网络服务中断或网络连接的带宽达到饱和，从而导致合法用户对某个特定的计算机或者网络资源不能正常访问。

DDoS 攻击中，仅仅一个小流量的慢速攻击，就可能消耗服务器大量的资源，甚至导致服务器崩溃。大流量及特大流量网络攻击则会导致数据中心总出口的链路拥塞，致使出口路由器设备单板转发异常，网络中继拥塞等，受影响的不只是被攻击的用户，还波及相当数量的其他用户。

原创医疗信息系统的数据中心出口需要部署 Anti-DDoS 设备进行安全防护。

### 9.4.3 Anti-Virus 网关

根据 ICSA 统计报告，磁盘传播的病毒仅仅占总病毒数的 1%，93%的病毒来自 email，2%的病毒来自 Internet 下载，另有 4%的病毒来自其它途径。随着全球经济运行对互联网的依赖，企业同时也面对着日趋升温的病毒侵扰，越来越多的企业考虑通过构建网络安全系统从整体上对企业的网络实行更为有效的多重防护。

传统的主机杀毒软件存在如下弊端，无法完全满足企业防病毒的需要。

——传统的主机杀毒软件不能在第一时间内查杀病毒，当病毒成功入侵企业网络后，扩散性和变异性使客户查杀变得十分被动和难以全面有效查杀。

——传统的主机杀毒软件并不能有效地抵御类似于 SQLSlammer 的新型蠕虫的功击。如果企业服务器站上的终端查杀软件未及时更新或被禁用，那么病毒仍然有机会感染企业服务器或和服务器相关的终端设备。

——主机杀毒软件会消耗较多的主机 CPU 资源，对于大业务量的数据中心服务器来说 CPU 资源非常宝贵。

——建议使用网络层的 Anti-Virus 网关对网络流量进行实时监控，发现恶意代码后实时阻断。部署 Anti-Virus 网关可根据需要串联或旁挂部署，通过双机热备部署来保证业务可靠性。Anti-Virus 网关可以做到以下几点：

——对外网发给内网的邮件进行病毒扫描，防止内部邮件服务器感染病毒。

——对外网用户上传 Web 服务器的文件进行病毒扫描，防止 Web 服务器感染病毒。

——保护服务器免受来自 Internet 的恶意攻击。

## 9.5 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：

——应对登录终端操作系统的用户进行身份标识和鉴别；

- 宜支持数字证书进行身份认证；

- 使用口令进行身份认证时，口令应有复杂度要求并定期更换。

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

——应对系统中的重要终端进行审计，审计粒度为用户级；

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

——审计记录至少应包括事件的日期、时间、类型、用户名、访问对象、结果等；

——应保护审计进程，避免受到未预期的中断；

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

——应定期对审计记录进行分析，以便及时发现异常行为；

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

——宜支持多操作系统，分离不同类型的应用场景；

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

## 9.6 应用安全

### 9.6.1.1 用户管理和权限控制

——应确保访问远程医疗信息系统的所有实体（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

- 对远程医疗信息系统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）。

——应根据用户对远程医疗信息系统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。

——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。

### 9.6.2 信息安全

#### 9.6.2.1 身份认证

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

- 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。

——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。

——应支持单点登录系统功能，用户只经过一次身份认证即可访问不同的业务系统

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

#### 9.6.2.2 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。

#### 9.6.2.3 关键业务抗抵赖

——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。

——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。

——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

#### 9.6.2.4 数据完整性保护

——应对交换数据进行数据完整性保护

- 宜采用数字摘要、数字签名技术保障数据的完整性。

——应对通信过程中的整个报文或会话过程敏感信息字段进行加密,系统应支持基于标准的加密机制：

- 宜采用 PKI 密码技术或采用具有相当安全性的其他安全机制实现。

——应保障交换数据的真实性及不可抵赖性

- 宜采用 PKI 密码技术或采用具有相当安全性的其他安全机制实现。

——应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。

——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。

### 9.6.3 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。

### 9.6.4 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。

### 9.6.5 审计追踪

——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。

——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。

——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；

——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。

### 9.6.6 管道安全

由于部分接入单位通过Internet连接地市中心的数据中心，要保证这些关键数据在传输过程中不被监听或者篡改，数据传输需要采用IPSec VPN加密技术传输。由于接入的卫生医疗机构众多，要保证接入单位能够同时接入，并保障设备可靠性。

### 9.7 数据安全及备份恢复

遵循《基于电子病历的医院信息平台技术规范》9.3.6。

## 10 性能要求

### 10.1 最小接入系统数

遵循《基于电子病历的医院信息平台技术规范》10.1。

### 10.2 最小并发用户数

遵循《基于电子病历的医院信息平台技术规范》10.2。

### 10.3 基础服务平均响应时间

遵循《基于电子病历的医院信息平台技术规范》10.3。

### 10.4 远程医疗数据资料整合服务平均响应时间

遵循《基于电子病历的医院信息平台技术规范》10.4。

### 10.5 远程医疗数据资料服务平均响应时间

遵循《基于电子病历的医院信息平台技术规范》10.5。

### 10.6 网络性能要求

#### 10.6.1 路由器性能要求

——支持 IPSec VPN 和 GRE VPN；
——支持信息中心监控设备：提供单板管理、电源管理、风扇管理、电子标签的信息监控功能；
——支持版本管理：提供在线版本升级、回退、补丁加载功能；
——支持镜像监控设备：提供基于端口和基于流分类的镜像功能；
——对于无线路有器需支持远程 PoE 供电：提供基于 LAN 侧的以太远程供电功能。

#### 10.6.2 交换机性能要求

——以太网接口可支持 10M、100M、1000M、10G 和自协商速率；
——支持接口流量控制，接口隔离、接口转发限制；
——支持广播风暴抑制；
——支持日志、告警、调试信息统一管理；
——支持设备自动加入集群；
——支持预防控制报文攻击；
——提供接口镜像、流镜像；
——支持 NAT 地址池、NAT 多实例；
——支持 AH 和 ESP 两种 IPSec VPN 模式。

#### 10.6.3 防火墙性能要求

——支持源 NAT、目的 NAT、源 PAT、目的 PAT 地址转换；
——可防范多种 DoS 攻击，包括 SYN Flood、ICMP Flood、UDP Flood、WinNuke、ICMP 重定向和不可达报文、Land、Smurf、Fraggle 等；
——可防范扫描窥探，包括地址扫描、端口扫描、IP 源站选路选项、IP 路由记录选项、ICMP 探测报文；
——支持电源 1+1 备份，支持电源热插拔；
——支持动态加载热补丁；
——支持基于应用层的流量控制，优先转发等 QOS 策略，保证重要的应用优先转发。

#### 10.6.4 入侵检测性能要求

——需支持分级管理，实现分布式部署、统一管理；
——可远程设置探测引擎环境、入侵检测规则及响应方式；
——要求实时跟踪当前的代码攻击；
——能够检测各种应用层攻击，包括但不限于：后门程序，木马程序，间谍软件，蠕虫，僵尸主机，异常代码，协议异常，扫描，可疑行为审计类等；
——能够对跨站攻击、SQL 注入等 WEB 攻击行为进行有效检测。