ICS
C07
备案号：

WS

中 华 人 民 共 和 国 卫 生 行 业 标准

WS/T XXXXX—2012

远程医疗信息系统基本功能规范

Basic functions specification of telemedicine information system

（送审稿）

2012 - XX - XX 发布　　2012 - XX - XX 实施

中 华 人 民 共 和 国 卫 生 部　　发 布

目 次

前 言

本标准由卫生部统计信息中心提出并归口。

本标准的主要起草单位：

本标准的主要起草人：

引 言

《远程医疗信息系统基本功能规范》是规范各地远程医疗信息系统建设的技术文件，对各区域远程医疗信息系统的应用服务子系统基本功能规范建设开展测试、验收和评价工作提供指导。

远程医疗信息系统基本功能规范

1 范围

本标准规定了远程医疗信息系统的总体技术要求、框架和基本功能要求，定义了远程会诊规范、双向转诊规范、远程预约规范、远程专科会诊规范、信息资源规范、安全规范和性能要求等，提出了提供远程医疗服务机构应遵循的功能和技术要求。

本标准适用于远程医疗信息系统的规划、设计、开发、部署和应用；建设单位可依据本规范对开发商提出建设要求。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/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 363-2011 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

WS XXX-2012 卫生信息共享文档规范

WS XXX-2012 基于电子病历的医院信息平台技术规范

电子病历基本架构与数据标准（试行） 卫办发〔2009〕130号

基于健康档案的区域卫生信息平台建设技术解决方案 （试行）卫办综发〔2009〕230号

信息安全等级保护管理办法 公通字［2007］43号

医院信息系统基本功能规范 卫办发 ［2002］ 116号

2010年远程会诊系统建设项目管理方案 卫办综函[2010]1046号

2010年远程医疗系统项目技术方案 卫办综函［2011］102号

3 术语和定义

下列术语和定义适用于本文件。

3.1

远程医疗信息系统 telemedicine information system

采用现代通讯、电子和多媒体计算机技术，实现医学信息的远程采集、传输、处理、存储和查询，对异地患者实施咨询、会诊、监护、查房、协助诊断、指导检查、治疗、手术、

教学、信息服务及其他特殊医疗活动的信息系统。

3.2

远程会诊 remote consultation

医疗机构之间利用远程医疗信息系统平台，采用离线或在线交互方式，对患者及其病史、检查等进行分析，完成病情诊断，确定进一步诊疗方案的医疗行为，包括远程专家会诊、远程心电诊断、远程影像诊断、远程病理诊断、远程重症监护等医疗服务。

3.3

远程会诊专家 experts of remote consultation

能够提供远程会诊服务的专家库成员，需具有副高以上专业技术职称，并专业五年（含）以上临床经验，近三年未发生过医疗事故；经本人审请，单位初审后报上级卫生主管部门审核批准，分为省级远程会诊专家和部级远程会诊专家。

3.4

远程心电诊断 remote electrocardiograph diagnose

基于远程医疗会诊系统由基层医疗机构向上级医疗机构提出申请并提供病人临床资料和心电资料，由上级医疗机构出具会诊意见及报告。包含高端远程实时心电监护。

3.5

远程影像诊断 remote medical image diagnose

基于远程医疗会诊系统由基层医疗机构向上级医疗机构提出申请并提供病人临床资料和影像资料，包括放射影像资料、B超影像资料以及视频资料，由上级医疗机构出具会诊意见及报告。

3.6

远程重症监护 remote intense care

基于远程医疗会诊系统由基层医疗机构向上级医疗机构提出申请并提供重症病人临床资料，包括实时在线的监护信息、放射影像资料、B超影像资料以及视频资料等，由上级医疗机构出具会诊意见及治疗指导意见。

3.7

远程病理诊断 remote pathology diagnose

基于远程医疗会诊系统由基层医疗机构向上级医疗机构提出申请并提供病人临床资料和病理资料，由上级医疗机构出具会诊意见及诊断报告。

3.8

远程手术示教 remote surgery demonstration

通过远程医疗信息系统的远程会诊技术和视频技术，对临床诊断或者手术现场的画面影像进行全程实时记录和远程传输，使之用于远程教学、远程观摩、远程诊断等。

3.9

远程医疗申请单 application for telemedical service

包括申请方医生姓名、职称、单位名称、医院等级、所属行政区域、申请目的与要求以及患者的症状、体征、主诉、实验室检查、影像学检查等资料。

3.10

患者、居民和个人 patient，resident，person

通过医疗卫生服务体系获取和接受服务的个体。

注：在本规范中这些术语可互换使用。

3.11

远程教育 distance education

在远程医疗信息~~会诊~~系统上，授课专家通过音视频和课件等方式为基层医生提供业务培训、教学以及技术支持。

3.12

远程医学数字资源 remote medical digital resource

上级医院收集整理的有典型意义的病例、案例分析、手术录像等资料，和与基层医疗机构共享的医学图书情报资源。

3.13

视频会议 video conference

两个或两个以上医疗机构，通过远程医疗信息系统的音视频传输和交互功能，达到即时且互动的沟通，以完成会议目的行为。

3.14

远程预约 remote booking

通过远程会诊系统远程预约功能，基层医疗机构的工作人员向上级医疗机构专家库成员提出预约申请，上级医疗机构处理预约申请，确定会诊时间的过程。

3.15

双向转诊 the two-way referral

医务人员根据患者病情治疗的需要，在上级和下级医疗机构之间实现转院的过程，基层医疗机构不具备患者病情治疗所需的技术和设备时，可以通过远程医疗信息~~会诊~~系统向上级医疗机构提出转院申请；上级医疗机构根据患者病情的治疗进展，认为无需在上级医疗机构继续治疗，可以将患者转到患者所在基层医疗机构继续治疗。

3.16

信息安全 information security

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。

4 缩略语

JPEG：一种图像格式（Joint Photographic Experts Group）

CDA：临床文档架构（Clinical document Architecture）

CIS：临床信息系统（Clinical Information System）

EHR：电子健康档案、健康档案（Electronic Health Record）

FTP：文件传输协议（File Transfer Protocol）

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

ID：标识号（Identity）

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

LED：发光二极管（Light Emitting Diode）

LIS：检验信息系统（Lab Information System）

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

PHSS：基层卫生服务系统（Primary Health Service System）

RIS：放射信息系统（Radiology Information System）

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

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

XML：可扩展标识语言（Extensible Markup Language）

GPRS：通用分组无线业务（General Packet Radio Service）

5 系统功能构成

5.1 系统分级

远程医疗信息系统的远程医疗服务包括9大子系统。其基本子系统包括远程会诊子系统、远程预约子系统、双向转诊子系统、远程影像诊断子系统、远程心电诊断子系统、远程教育子系统；高端远程医疗服务子系统，包括远程监护子系统、远程手术示教子系统、远程病理诊断子系统等高端远程会诊服务子系统。

5.2 功能结构图

远程医疗信息系统是在统一的数据中心基础上构建的应用服务系统，其应用服务功能包括远程会诊、远程预约、双向转诊、远程专科诊断、远程监护和远程手术示教等功能，其数据中心基本功能包括医疗单位管理、专家资源库管理、患者资料管理、用户管理、费用管理、以及数据字典管理等服务，可以通过接口与临床信息系统（CIS）、医院信息系统（HIS）、医院检验系统（LIS）、放射信息系统（RIS/PACS）和基层卫生服务系统（PHSS）等系统进行信息共享，整个功能结构如图1所示：

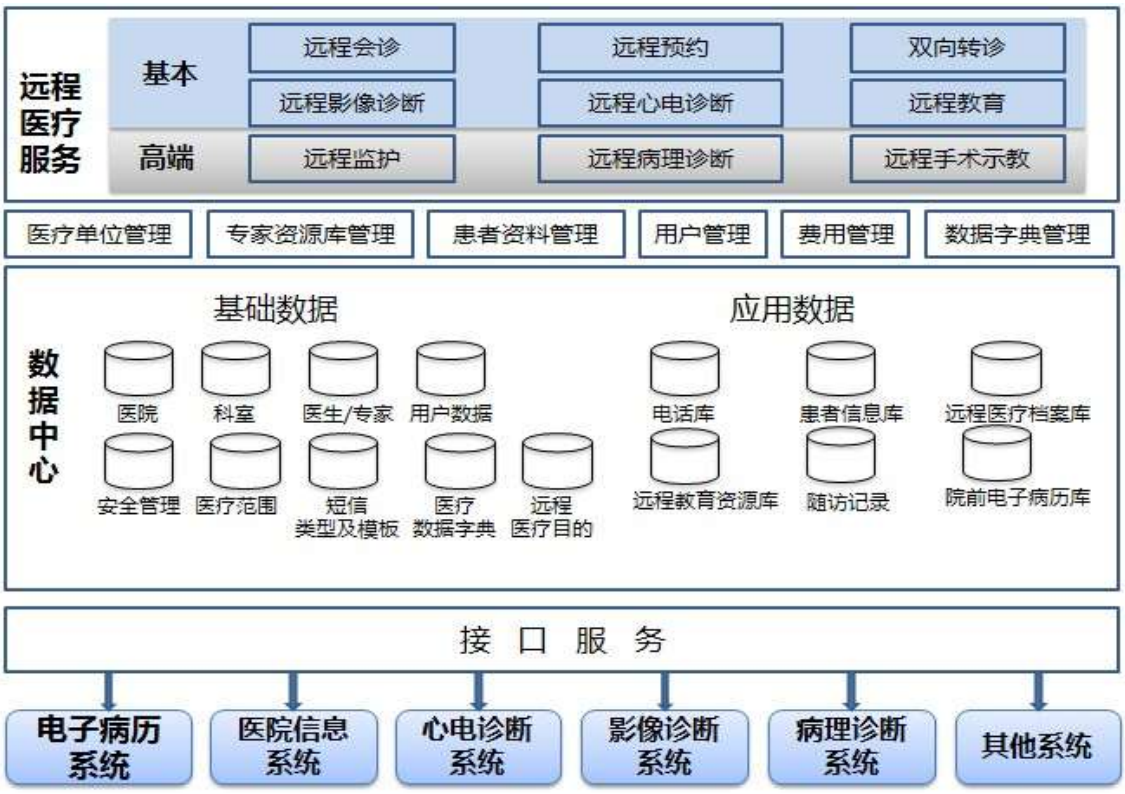

图1 远程医疗信息系统功能架构图

6 功能要求

6.1 远程医疗基本功能

6.1.1 远程会诊

6.1.1.1 适用范围

适用于基层医务人员或医疗机构向上级医务人员或医疗机构的远程会诊申请，专科医院和综合性医院之间提出的相互会诊请求。

6.1.1.2 基本功能

——会诊申请：会诊申请单的填写、会诊申请提交与修改、专家库信息查询、患者病历资料提交与查询、会诊申请的查询、会诊报告的查询等；

——会诊管理：会诊流程管理、病历资料管理、会诊报告浏览、随访管理等；

——专家会诊：病历资料浏览（医学影像、心电、病理图片等）、会诊报告编写、修改与发布、会诊报告模板管理、会诊服务评价等。

6.1.2 远程预约

6.1.2.1 适用范围

适用于基层医院完成预约挂号、预约检查等操作；支持上级医院完成相关申请受理及信息反馈。

6.1.2.2 基本功能

——预约机构和排班表的管理：对远程预约的医疗机构进行管理登记、建立远程预约协议；

——预约申请：预约申请单的填写、排班表查询和号源选择、预约申请提交与修改、患者病历资料的提交、预约单的浏览和打印等；

——预约管理：预约过程管理、预约过程提醒、预约记录查询、预约流程管理、病例资料管理等。

6.1.3 双向转诊

6.1.3.1 适用范围

适用于基层医疗卫生服务机构对转入、转出病患者的管理过程。

6.1.3.2 基本功能

——转诊定点机构管理：对各类疾病的转诊医疗机构进行管理登记、建立转诊协议；

——转诊申请：响应全科诊疗、其它服务组件或系统模块的转诊请求，向定点转诊机构提出转诊申请。具备转诊申请单填写、转诊申请的提交与修改、接诊机构查询、转诊申请的查询等功能；

——转诊管理：分为送转管理和接诊管理，支持送转方进行取消送转、打印转诊单、重新转出操作；支持接诊方进行接诊或拒绝接诊操作。具备转诊过程管理、病例资料管理、转诊过程提醒、转诊记录查询等功能；

——自动转诊：出院病人信息都可从医院的HIS系统中自动获取；根据转诊记录信息自动转回原送转机构，或根据病人地址信息转回该病人被管辖的社区医疗机构；

——随访功能：包括随访记录和随访计划、随访记录查询和随访提醒等。通过双向转诊，社区卫生服务机构能实时知晓所辖地区内的所有出院病人信息，并进行主动随访与院后管理，指导病人用药和康复，引导病人就地复查复诊，控制病情复发。

6.1.4 远程影像诊断

6.1.4.1 适用范围

适用于基层医务人员或医疗机构向上级医务人员或医疗机构的远程影像诊断申请，以及

区域内多家医疗机构联网组成影像中心，对影像的集中存储和管理。

6.1.4.2 基本功能

——权限管理：要求对多家医院的用户权限进行严格多级设置管理：支持对多个医院的权限进行授权分配，支持对医院的不同影像检查的报告诊断与浏览等权限的分配，支持对不同影像检查的书写、审核、修订及浏览等权限的分配，所有密码必须加密保存和传输；

——报告诊断和浏览；

——集中存储：所有接入医院的患者检查信息、检查申请单信息、相应的检查证据文本等集中存储到区域检查数据仓库，进行统一调阅、统一管理，实现检查数据共享。支持患者基本信息与检查信息的采集录入、病例类型归档、备注信息，支持灵活多样的检索方式，支持病理自动追踪与病理诊断报告查阅，支持上传与调阅扫描申请单或电子申请单等；

——集中质控：建立影像读片资料库；建立各医院的阅片质量追踪数据库；统一的传染病统计和报卡服务。应实现的基本功能包括：影像质量统计、技师评片、集体评片、报告书写质量统计、技师的影像总体质量统计、诊断报告诊断质量统计、疾病智能报卡与统计等；

——病例学习：为医师提供一个学习提高的平台，特别是一些进修医师与实习生，可以对其关心的报告进行查询浏览并进行对比学习与收藏。

6.1.5 远程心电诊断

6.1.5.1 适用范围

适用于基层医务人员或医疗机构向上级医务人员或医疗机构的远程心电诊断申请，以及院前 120 急救中心心电检查需求。

6.1.5.2 基本功能

——登记：接受患者的预约登记和检查登记，以及对患者检查信息的登记，申请单扫描和简单查询统计（如患者列表，个人工作量，检查人次和收费金额等），并分发患者的检查报告。具备为病人分配预约时间、查询指定时间段内的预约、登记病人列表、纸介质申请单的扫描和拍摄、与HIS系统无缝对接等功能；

——采集：采用数字心电图接口技术，将心电图机数据转换成标准通用心电图数据，发送到心电中心服务器，实现全院医生临床web浏览。支持心电图采集、存储、回放与传输功能；

——分析诊断：专业心电医生根据心电设备采集的数据进行专业分析诊断。具备心电检查数据到达即时提醒、心电图分析、报告编写和打印、病例管理等功能；

——心电管理：主要是区域心电信息系统的人员管理和基础数据字典的管理；

——报告浏览：给临床医生提供浏览心电图报告及心电波形的工具。可将医生端浏览工作站嵌入到门诊医生工作站、住院医生工作站和电子病历系统中去，支持医生端浏览工作站可进行在线波形分析、处理、测量功能。

6.1.6 远程教育

6.1.6.1 使用范围

适用于医院、专家通过音视频和课件等方式为基层医生提供业务培训、教学、病案讨论以及技术支持。

6.1.6.2 基本功能

——课程查询：具备课程视频查询、视频点播、实时培训及课件同步等功能；
——课程学习：具备课程学习计划制作、课程培训记录、学习进度查询等功能；
——课程管理：具备视频管理、课件管理、视频共享等功能；
——学分管理：具备申请学分、学分证打印等功能。

6.2 高端远程医疗服务

6.2.1 远程监护

6.2.1.1 概述

通过远程医疗信息系统，远程监护申请经会诊中心同意后，基层医院的危重患者在病床上实时接受远程专家的监护服务，支持床边呼吸机、监护仪等生命体征数据的实时采集和传输，实现对患者病情的24h不间断的连续、动态观察。远程监护是远程医学的重要组成部分。远程监护是在远程会诊基础上，在专家方和申请方之间开展持续3d以上监护、交班、治疗的医疗活动。

6.2.1.2 基本功能

——具备实时采集传输床边呼吸机、监护仪等生命体征参数功能，申请方、专家方、患者之间进行持续动态监护、诊断建议、治疗建议等医疗活动；
——具备24h不间断的连续动态观察，向专家方提供患者实时持续的监护数据（心率、血压等），并对异常情况预警和警报作用；
——具备生命体征参数的存储、管理等功能常规功能，也包括数据记录、管理、查询、统计功能；
——具备患者床边视频会议功能，便于专家与申请医生和患者远程互动式交流；
——具备专家远程实时控制视频云台，对患者多角度观察和画面快速切换；
——申请方可以进行远程会诊、查房、病例讨论等医疗行为；

6.2.2 远程病理诊断

6.2.2.1 概述

基层医疗卫生机构由于设备条件落后或不具备该技术，可以通过远程医疗信息系统向上级医疗机构提出远程病理诊断请求，上级医疗专家根据申请内容和申请医生提供的病理资料进行会诊，并做出会诊意见，对下级医疗卫生机构给技术支持。

6.2.2.2 基本功能

——具备病理切片数字化扫描功能，病理切片转换成数字切片；
——具备虚拟数字切片的放大、缩小、标记等后处理功能；

——具备病理图文报告的书写、发布、保存以及记录查询等功能；

——具备患者信息上传、报告下载等功能。

6.2.3 远程手术示教

6.2.3.1 概述

通过远程医疗信息系统的远程会诊技术和视频技术，对临床诊断或者手术现场的画面影像进行全程实时记录和远程传输，使之用于远程教学、远程观摩、远程诊断等。

6.2.3.2 基本功能

——具备一个手术室可以支持多个远程教室同时观看手术过程的功能；

——具备医学专家可以在局域网任意点连接同一个手术室或连接多个手术室，进行手术指导和讨论的功能；

——具备对手术影像和场景视频进行全程的实时记录功能；

——具备对手术过程静态拍照和动态录像的功能；

——具备对手术高质量音视频存储、回放和管理等功能；

——具备手术实况音视频信息实时直播、刻录的功能；

——具备手术室和医学专家实时交互的音视频通话的功能；

——具备术野图像监看高清电视或LED电视；

——具备术野摄像机远程微控功能；

——具备术野摄像机和手术室内其他摄像机远程云台控制功能。

6.3 数据管理

6.3.1 概述

数据管理包括基础数据和应用数据，是对各级医疗机构、医务人员以及患者信息资源进行统一管理，并与其它各个功能子系统对接，实现基础数据和应用数据的存储、交换、更新、共享以及备份等功能，实现远程医疗服务。

6.3.2 基本功能

6.3.2.1 医疗卫生机构数据管理

建立远程医疗信息系统的医疗卫生机构信息库，其基本功能包括：

——具备医疗卫生机构的注册功能；

——具备医疗卫生机构的信息浏览功能；

——具备医疗卫生机构的信息删除功能；

——具备医疗卫生机构等级管理功能；

——具备医疗卫生机构类型管理功能。

6.3.2.2 科室数据管理

建立远程医疗信息系统的科室信息库，其基本功能包括：

——具备科室的注册功能；

——具备科室的信息浏览功能；

——具备科室关联功能；

——具备医院学科管理功能；

——具备重点科室类型管理功能。

6.3.2.3 专家数据管理

建立远程医疗信息系统的医院信息库，其基本功能包括：

——具备专家的注册功能；

——具备专家的信息列表浏览功能；

——具备专家资料的管理功能；

——具备专家临床职称管理功能；

——具备专家教学职称管理功能；

——具备专家其他职称管理功能；

——具备专家学历管理功能；

——具备专家证件管理功能。

6.3.2.4 病历数据采集

采集患者病历信息，其基本功能包括：

——模拟信号处理：患者的胶片及纸质病历、化验单、图文报告等通过扫描方式实现数字化；支持扫描文件的传输、存储和阅读，扫描文件以JPEG格式，胶片资料以DICOM3格式，支持病历资料的手工录入；

——数字信号处理：支持借助DICOM网关从具有DICOM3接口的影像设备获取患者的影像资料，支持从PACS图文工作站导入DICOM3影像。支持与电子健康档案、电子病历、数据中心等系统间实现互联互通。有条件的医院可以根据卫生部已经颁布的有关电子病历的标准规范，导出患者病历信息，远程会诊系统支持针对导出信息的导入、传输、存储和阅读；

——实时生命体征信号的处理：支持床边呼吸机、监护仪等生命体征数据的实时采集与传输，实现对患者进行24h不间断的连续、动态观察。

6.3.2.5 随访数据服务

会诊中心根据会诊记录定期进行随访以提高会诊质量，其基本功能应包括：

——具备随访类型管理功能；

——具备随访方式管理功能。

6.3.2.6 统计分析

通过数据管理可以对日常数据进行报表统计和查询，基本功能应包括：

——远程会诊申请、患者病历、专家信息、意见与随访记录的查询功能和会诊数量和专家工作量的统计功能；

——远程预约情况以及响应其他服务组件、功能模块的查询统计功能；

——双向转诊信息的查询、调阅、使用与送转接诊、上转下转、送转病人按类型和接诊病人按类型统计的功能，以及响应其他服务组件、功能模块要求的查询统计功能；

——具备向各医疗机构和管理人员提供影像资料、患者病历、影像会诊情况的查询和统计功能；

——具备向各医疗机构和管理人员提供心电资料、患者病历、心电会诊情况以及阳性率、检查费用、会诊工作量的查询和统计功能；

——具备远程教育不同类型视频、视频名称模糊搜索以及个人培训视频记录的查询功能和视频类型、点播次数及系统课程的统计功能。

6.3.2.7 财务管理

——具备收款通知与确认管理功能；

——具备医院对账单管理功能；

——具备专家费用支出签收单据管理功能；

——具备根据不同省市级别设置收费标准功能；

——具备费用结算清单管理功能，包括医院费用、申请医生费用、会诊专家费用等总计功能；

——具备申请医生、专家费用和运营费用比例设置功能；

——具备制作费用统计报表功能，包括省份、地级市、县区级和医院级别的总计功能；

——具备制作收款和支付费用月、年度报表功能，包括省份、地级市、县区级和医院级别的年度总计功能。

6.3.2.8 功能协作与数据交互

——具备与电子病历、HIS系统、区域卫生信息系统、视频会议系统等其他医疗信息化系统协作完成患者病历资料、远程会诊结果、转诊预约、影像心电资料、视频调用浏览的相互查询、记录和使用等功能；

——通过与医院HIS、EMR、社区EHR、视频会议系统、医保系统、区域卫生信息平台等系统的接口，实现其数据交互，接口功能包括：病历资料获取、会诊结果导入、预约申请登记、预约结果反馈、转诊申请登记、转诊接收、与遵循国际标准的第三方厂商的影像、心电系统的集成、视频点播、信息浏览等。

7 系统总体要求

7.1 可操作性

系统应考虑实用性与先进性相结合，要体现出易于理解掌握、操作简单、提示清晰、逻辑性强，直观简洁、帮助信息丰富，而且要针对医疗卫生行业输入项目的特点对输入顺序专门定制，保证操作人员以最快速度和最少的击键次数完成工作。

系统功能设计合理，易于操作使用，有电脑及软件基础知识的人员，无须经过专业培训，即可快速掌握软件操作；系统提供联机帮助说明，提供软件操作的电子文档说明书，方便用户使用。

7.2 安全性

系统的安全体系由权限管理、日志审计和安全机制构成，既要实现信息资源的合理共享，又支持信息的保护和隔离；对系统数据的存取和改变进行严格的控制，对系统数据进行有效的保护，以杜绝数据的非法操作和防止计算机病毒的破坏。当使用本系统时，系统先进行用户的识别和鉴定，可让用户输入标识或口令进入并设置好各用户的相应权限，保证用户只能存取他有权存取的数据。

7.3 可靠性

系统应该可实现7×24小时连续安全运行，性能可靠，易于维护。有严密的用户权限的管理和控制。要求系统在发生故障或输入数据不合理的情况下，有较高的抗干扰能力和控制故障的能力，以免系统发生停顿或遭到破坏而影响工作。平台在瘫痪后能够在短时间内迅速恢复，应有相应的检修和自动恢复功能。平台在用户出现错误操作时能进行提示，并自动停止该操作。

7.4 可扩展性

系统建设过程中遵循扩展性原则，系统必须提供标准的开发接口与用户现有或将来扩展的业务系统集成，特别要加强系统设计的前瞻性、预留系统扩充和扩展能力。

7.5 开放性与兼容性

各子系统应模块化，并完全兼容第三方系统，各功能模块之间的通讯采用标准通讯协议（如TCP/IP)而非专有技术，系统应该采用通用的数据库平台，通信平台统一使用成熟技术，支持使用通用的PC和通用的系统下运行。

8 信息安全与隐私服务

8.1 用户管理和权限控制

8.1.1 实体认证

——应确保访问区域卫生信息平台的所有实体（用户和系统）采用唯一身份标识，并对实体身份进行统一管理：

- 对区域卫生信息平台各类实体信息进行数字身份的定义和标识；
- 实现数字身份流程化管理，控制数字身份的整个生命周期，支持身份信息申请、审批、变更及撤销等管理操作；
- 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。

8.1.2 实体授权

——应根据用户对区域卫生信息平台系统的使用性质的不同进行用户分类管理：

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

——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。

8.1.3 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：

——标识和鉴别系统用户的过程：应符合功能8.1.1（实体认证）；

——角色的职能分割：应符合功能8.1.2（实体授权）；

——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。

8.2 信息安全

8.2.1 病人访问管理

——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8.1.1（实体认证）；

——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8.1.2（实体授权）；
- 应符合功能8.1.3（实体访问控制）；

8.2.2 不可抵赖

——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。

8.2.3 数据安全传递

——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8.1.1（实体认证）；

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

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

——应保障交换数据的真实性及不可抵赖性：应符合功能8.2.2（不可抵赖）。

8.2.4数据安全路由

——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；

——应确保只和认证及授权过的来源和目的地进行患者临床资料的数据传递：

- 应符合功能8.1.1（实体认证）；
- 应符合功能8.1.2（实体授权）；
- 应符合功能8.1.3（实体访问控制）；

——应保障传递数据的安全性：应符合功能8.2.3（数据安全传递）。

8.2.5信息验证

——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；

——应提供患者临床资料的编写者进行增加和修改患者临床资料的内容；

——应提供患者临床资料的编写者进行患者临床资料的验证功能：

- 宜采用数字签名/验签技术实现；
- 应标明患者临床资料是否被验证；
- 验证过程记录的文件要有保留。

——能够为通过认证和授权的用户情况提供患者临床信息的验证：

- 应符合功能8.1.1（实体认证）；
- 应符合功能8.1.2（实体授权）；
- 应符合功能8.1.3（实体访问控制）。

8.3 隐私保护

——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8.1.1（实体认证）；
- 应符合功能8.1.2（实体授权）；
- 应符合功能8.1.3（实体访问控制）；
- 应符合功能8.2.2（不可抵赖性）；
- 应符合功能8.2.3（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。

——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；

——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患者临床资料或者在紧急治疗情况下不经许可直接开放患者临床资料。

8.4 审计追踪

——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；
- 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，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。