ICS 35.240.80
CCS C 07

团　　体　　标　　准

T/CIIA XXXX—XXXX

定点医疗机构医疗保障基金监管系统技术要求

Medical security fund supervision system of designated medical institutions—Technical requirements

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国信息协会　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由中国信息协会提出并归口。

本文件起草单位：

本文件主要起草人：

定点医疗机构医疗保障基金监管系统
技术要求

1 范围

本文件规定了定点医疗机构医疗保障基金监管系统的系统架构、功能要求、性能要求、数据要求、接口要求、安全要求以及运维要求。

本文件适用于定点医疗机构医疗保障基金监管系统的建设与运行。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件；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 7408 数据元和交换格式 信息交换 日期和时间表示法

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 39786 信息安全技术 信息系统密码应用基本要求

GB 50174 数据中心设计规范

GB 50462 数据中心基础设施施工及验收规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

医疗保障基金监管系统 medical security fund supervision system

用于监督、管理和审核医疗保障基金的支出和使用情况的计算机系统。

3.2

稽核管理 audit management

对医疗保险的缴费情况、医疗费用支付及使用情况等进行检查和审核的过程。

4 缩略语

下列缩略语适用于本文件。

IP：网际互连协议（Internet Protocol）

Web：全球广域网（World Wide Web）

JSON：JS对象简谱（JavaScript Object Notation）

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

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

API：应用程序编程接口（Application Programming Interface）

VPN：虚拟专用网络（Virtual Private Network）

URL：统一资源定位符（Uniform Resource Locator）

SSL：安全套接层（Secure Sockets Layer）

TLS：传输层安全性协议（Transport Layer Security）

5 系统架构

定点医疗机构医疗保障基金监管系统架构宜参见图1。

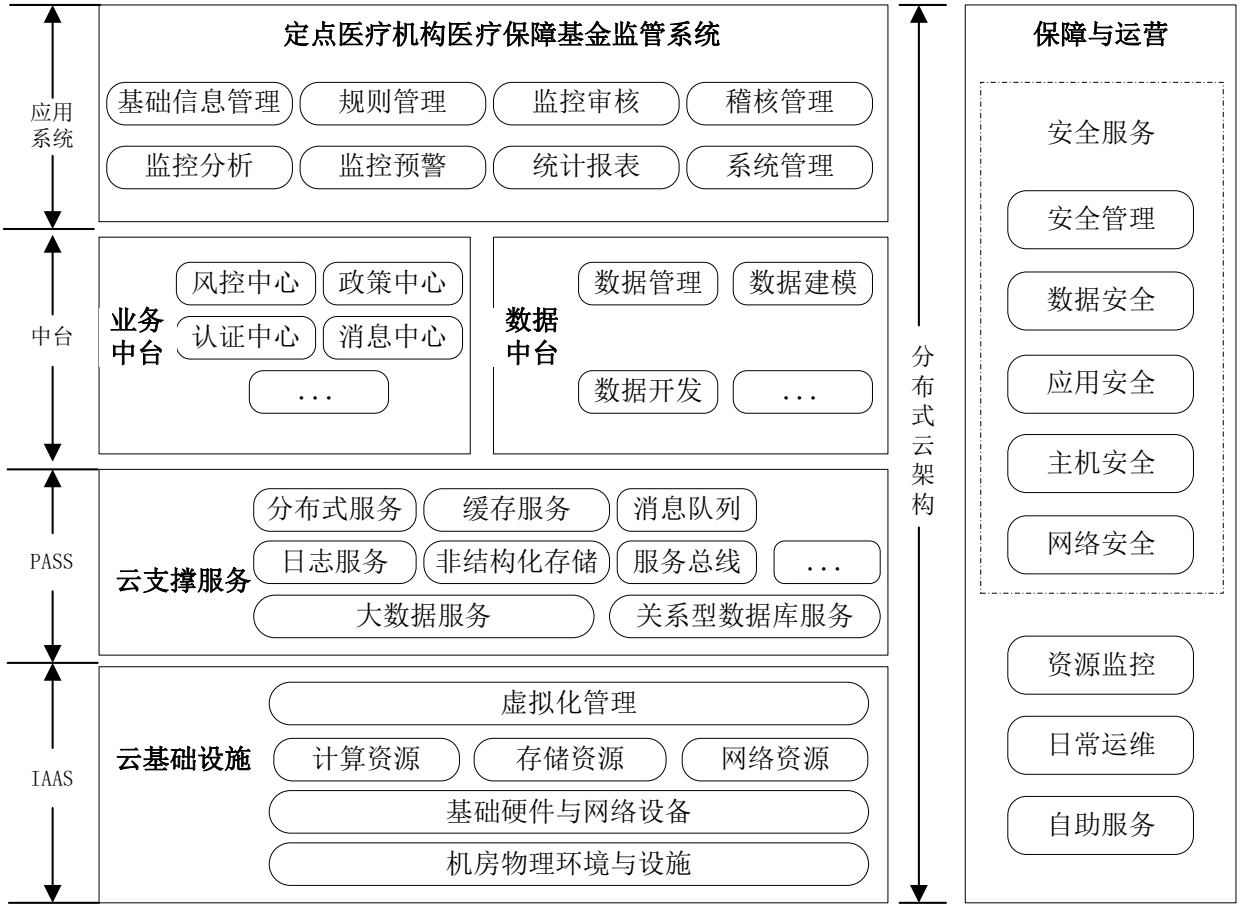

图1　定点医疗机构医疗保障基金监管系统架构

6　功能要求

6.1　基础信息管理

基础信息管理包括但不限于以下功能：

a)　医疗机构信息管理；
b)　患者信息管理；
c)　药品信息管理；
d)　费用信息管理；
e)　医嘱和处方信息管理。

6.2　规则管理

规则管理包括但不限于以下功能：

a)　规则维护：
　　1)　应提供规则列表，方便用户对规则进行管理和操作；
　　2)　应支持用户对规则进行新增、编辑、删除、查询、启用和停用等功能；
　　3)　应支持用户定制监控规则，针对不同监控对象和场景进行修改和调整。
b)　创建计划任务：
　　1)　应支持创建计划任务功能；
　　2)　应支持用户对计划任务进行新增、编辑、删除、查询、启用和停用等。
c)　执行方案配置：
d)　应支持根据业务需求设定一系列自动执行的任务、规则及其触发条件的执行方案配置功能。

1） 应支持用户对执行方案进行新增、编辑、删除、查询、启用和停用等。

e） 任务规则配置：

1） 应支持任务规则配置功能；

2） 应支持用户对分析规则进行新增、编辑、删除、查询等。

f） 执行结果跟踪：

1） 应支持执行结果跟踪功能；

2） 应支持查询计划或方案的执行结果，并提供执行日志；

3） 用户可根据条件检索执行结果，方便筛选和查找相关信息。

6.3 监控审核

监控审核包括但不限于以下功能：

a） 违规汇总审核：对系统中检出的所有类型的规则进行统计与初审，分为三个维度（参保人、医生、医院等）审核规则的集中汇总，方便医院监管人员进行审查；

b） 执业医师审核：对系统中检出的所有执业医师违规的规则进行统计与初审，主要以医师为主要因子进行排序，利用医保管理知识库、临床诊疗规范知识库和药品知识库，监控医院医师诊疗行为的合理性；

c） 违规数据浏览：用户可查看违规患者列表和基本信息；

d） 查询功能：支持用户通过不同的查询条件来检索违规规则；

e） 界面功能：提供标记、导出以及更多信息查看等功能；

f） 诊疗数据处理：用户可查看违规详细信息，并进行疑点记录、原始单据、治疗方案等方面的查看和处理。

6.4 稽核管理

稽核管理包括但不限以下功能：

a） 稽核任务创建：用户可在稽核任务创建界面新增任务，添加待稽核的规则，并提交修改后发布任务；

b） 稽核任务跟踪：用户可通过稽核任务跟踪界面编辑任务状态，包括对任务状态进行修改，以及对稽核状态、稽核结果和处罚结果进行编辑；

c） 稽核结果查阅：用户可按任务、规则或案例（系统稽核过程中发现的具体问题或违规行为的实例）进行稽核结果查询。按任务查询时，可以查看相关的规则记录和稽核描述列表；按规则查询时，显示稽核描述列表；按案例查询时，显示具体的稽核任务描述信息。

6.5 监控分析

监控分析包括但不限以下功能：

a） 机构费用增长幅度分析：支持查看不同定点医疗机构的医疗费用占比，并分析环比增长幅度和机构类别费用排名；

b） 机构交易量分析：支持查看当月定点医疗机构的交易总金额和交易总人次，分析月交易量趋势和日交易量趋势，并查看交易明细；

c） 门特就诊分析：支持查看各定点医疗机构当月门诊大病就诊人数、人次数、就诊总费用以及增长幅度的对比和环比，分析均次费趋势；

d） 参保类型分析：支持查看不同类型的参保人员的医疗总费用占比，根据所选择的参保类型，统计该类型门诊、住院均次费用，以及基金支出门诊、住院均次费用并通过柱状图对多个月情况进行对比；

e） 医保总费用分析：支持查看医保总费用分析，包括按月分析和按人员类别分析等；

f） 机构均次住院费用分析：支持查看定点医疗机构均次住院费用分析，包括具体记录和相关柱状图展示。

6.6 监控预警

监控预警应支持对基金运行状况的相关指标配置风险阈值，并设定风险级别，利用大数据分析模型或算法，对医保费用进行多维指标分析，识别医疗机构、科室、医师或患者在医疗服务过程中的异常情况，进行不同程度的预警，具体预警阶段包括：

a) 事前预警：在医生通过 HIS 系统为患者开具处方或开立医嘱时，对处方（医嘱）中超临床规则和超医保规则的处方进行实时分析并给予警示，一旦出现超临床规则、超医保规则的药品或项目异常，系统将实时发出警示，减少或避免处方中的不合理用药行为、处方中的违规诊疗行为；
b) 事中监控：对在院病人每日预结算数据进行分析，将直接违规行为或违规疑点信息推送给具体科室公示，临床科室核对并整改，医嘱医生如有异议的直接违规行为或疑点提交说明材料；临床科室未进行整改、未提交说明的违规行为或违规疑点在患者住院预结算审核中发现将对该科室及具体违规医生进行绩效扣罚；
c) 事后审核：针对门诊和住院患者在离院后的诊疗数据，从行为和项目维度进行分类审核，以单据维度展现违规信息，并结合统计分析工具发现医疗机构管理漏洞。

6.7 统计报表

统计报表模块包括但不限于以下功能：

a) 应支持对统计报表的生成、管理、更新、查询和删除；
b) 应支持对基础数据、专题数据、政策数据的统计分析；
c) 应具有多级院内数据上报报表体系。

6.8 系统管理

系统管理模块包括但不限于以下功能：

a) 用户管理；
b) 角色管理；
c) 模块管理；
d) 权限管理；
e) 日志管理。

7 数据要求

7.1 基本属性

系统平台数据元的实体和元素描述属性见表1。

——描述属性：描述数据元实体和数据元元素的属性。

——要求：描述数据元实体和数据元元素的该属性是必备属性还是可选属性。

——定义及说明：对描述属性的说明。

表1 数据元描述属性

序号	描述属性	要求	定义及说明
1	中文名称	M	数据元实体和数据元元素的中文名称
2	英文名称	O	数据元实体和数据元元素的英文名称
3	数据类型及格式	M	数据类型：对数据元实体和数据元元素的有效值域和允许对该值域内的值进行有效操作的规定
4	值域	O	数据元元素所允许的值的集合
注：“M”是“Mandatory”的缩写，表示必备属性；“O”是“Optional”的缩写，表示可选属性。			

7.2 数据类型及格式

7.2.1 数据类型

数据元实体的数据类型为复合型，数据元元素的数据类型表示方法见表2。

表2 数据类型表示方法

序号	数据类型	表示方法	说明
1	字符型	C	可以包括字母字符、数字字符或汉字等在内的任意字符
2	数值型	N	数值
3	日期型	YYYYMMDD	格式按GB/T 7408中的规定，“YYYY”表示年，“MM”表示月，“DD”表示日
4	时间型	hhmmss	格式按照GB/T 7408中的规定，“hh”表示时，“mm”表示分，“ss”表示秒
5	日期时间型	YYYYMMDDhhmmss	格式按照GB/T 7408中的规定
6	布尔型	B	y/n
7	二进制流型	BY	图像、音频、视频等二进制流文件格式

7.2.2 数据格式

数据元元素的数据格式的标识方法如下：

a） 字符型和数值型后加正整数表示定长格式；

示例1：C6 表示 6 位定长的字符。

示例2：N16 表示 16 位定长的数值。

a） 字符型和数值型后加“x..y”表示从最小到最大长度的格式；

示例3：C..10 表示最短 1 位、最长 10 位的字符。

示例4：N..6 表示最短 1 位、最长 6 位的数值。

b） 字符型后加“..ul”表示长度不确定的格式；

示例5：C..ul 表示长度不确定的字符，一般多为大量的文本内容。

c） 数值型后加“x,y”表示小数位；

示例6：N..17,2 表示最长 17 位的数值，其中小数点前 14 位、小数点 1 位、小数点后 2 位。

d） 二进制流型后加具体的媒体格式。

示例7：BY-JPEG 表示“JPEG”格式的文件。

8 接口要求

8.1 设计原则

接口设计的基本原则包括但不限于：

a） 安全性原则：应提供多种安全可靠的技术手段（加密技术、身份验证与授权、访问控制等），以保证接口数据的安全；

b） 开放性原则：应采用通用的接口设计标准，保证与其他系统的互联互通；

c） 灵活性原则：应能根据业务变化，灵活调整接口容量与性能；

d） 松耦合原则：应避免提供方的业务系统对接口服务实现的依赖性；

e） 信创兼容性原则：宜考虑信创环境下的技术栈和生态，确保接口能够兼容信创软硬件产品。

8.2 基本要求

8.2.1 接口要求

8.2.1.1 硬件接口

硬件接入应提供物理设备的接口，包括但不限于：

a） 服务器设备；

b） 网络设备；

c） 存储设备。

8.2.1.2 软件接口

软件接入要求：

a） 系统应提供 RESTful 或 SOAP 等标准的 Web 服务接口，以支持跨平台、跨语言的应用集成和数据交互等；

b) Web 服务接口应具有良好的可扩展性和灵活性，允许根据实际需求定制和调整接口参数和数据格式；
c) 应提供系统使用单位相关的增、删、改、查等接口；
d) 应提供云主机的相关接口，包括虚拟机云主机详细信息、列表、快照、硬盘规格、镜像等；
e) 应提供存储资源相关的接口，包括云硬盘、硬盘快照、访问鉴权等；
f) 应提供虚拟网络资源相关的接口，包括网络、子网、网卡、虚拟路由、安全组、公网 IP、VPN 等。

8.2.1.3 云平台接口

应提供云管理平台的开放接口，以实现定点医疗机构医疗保障基金监管系统能够被第三方应用开发、部署和安全监管，包含但不限于：

a) 提供丰富的 REST API 接口供第三方在云操作系统上进行业务应用开发部署，提供的接口涵盖基础设施、支撑软件和业务应用各个层面，实现一个开放的定点医疗机构医疗保障基金监管系统；
b) 提供多种安全监管接口，以提供相关安全监管数据。安全监管接口类型包括网络流量接口、网络协议接口、云主机接口和 API 等。

8.2.2 调用方式

8.2.2.1 应使用 HTTP 或 HTTPS 协议进行接口调用，确保数据传输安全可靠。
8.2.2.2 应根据操作类型选择合适的 HTTP 请求方法，如 GET、POST、PUT、DELETE 等，确保操作的语义清晰。
8.2.2.3 接口 URL 应明确主机地址、端口号（可选）、接口路径等部分，以反映接口的功能和用途。
8.2.2.4 参数传递要求如下：

a) GET 请求应将参数附加在 URL 的查询字符串中。
b) POST 请求应将参数放在请求体中，通常使用 JSON 或表单形式。
c) 对于涉及安全性的敏感数据，应当使用 HTTPS 进行传输，并对参数进行加密处理。

8.2.2.5 应使用 API 密钥或 Token 进行身份认证，确保只有授权的用户或系统能够访问接口。
8.2.2.6 返回数据要求如下：

a) 接口注册时应标明接口的返回格式；
b) 返回数据应采用固定的格式封装，如 xml、JSON 等；
c) 接口调用不通过，可通过返回码返回数据，接口调用返回错误定义类型见表 3。

表3 接口调用返回错误定义类型

序号	说明
1	调用超时
2	服务器处理失败
3	用户已被禁用
4	用户表服务被禁用
5	服务还不能开始使用
6	服务使用过期
7	表服务码不能为空
8	用户没有授权该数据服务
9	验证码错误
10	用户名或密码错误
11	未登录或登录超时，请重新登录
12	未输入参数或参数格式有误
13	没有当前查询信息

14	除上述内容外的源网实际回信
15	请求发生异常

8.2.2.7 应记录接口调用的相关信息，包括调用时间、调用方身份、请求参数、响应结果等，方便日后排查问题和系统监控。

8.3 接口描述

8.3.1 依赖中台接口

定点医疗机构医疗保障基金监管系统应支持向其他中台（风控中心、统一认证中心、基础信息中心、用户中心等）提供数据查询、新增、更新、删除等功能。

8.3.2 依赖子系统接口

定点医疗机构医疗保障基金监管系统应支持向其他子系统（医保业务基础子系统、医疗服务价格管理子系统等）提供标准化接口。

8.3.3 对外服务接口

定点医疗机构医疗保障基金监管系统应向外部系统或服务提供标准化接口，以实现数据交换、信息传递或业务流程的协同。

9 安全要求

9.1 访问控制

定点医疗机构医疗保障基金监管系统的访问控制具体要求如下：

a) 应实现严格的用户身份验证机制，包括用户名和密码验证，并采用多因素身份验证；
b) 应设定不同用户角色，并基于角色进行权限控制，确保每个用户只能访问其权限范围内的数据和功能；
c) 应实施登录失败次数限制和登录尝试频率限制。

9.2 数据保护

定点医疗机构医疗保障基金监管系统的数据保护具体要求如下：

a) 应符合 GB/T 22239 中不低于等保三级的关于安全审计、可信验证、数据完整性、数据机密性、数据备份恢复、剩余信息保护、个人信息保护的规定，并按照 GB/T 39786 中不低于等保三级的应用和数据安全要求执行；
b) 应使用加密技术保护数据的传输和存储，在数据传输过程中采用 SSL/TLS 协议加密通信；
c) 应采用数据备份和恢复机制，定期备份数据；
d) 应设立数据访问审计机制，记录用户对敏感数据的访问和操作。

9.3 漏洞管理

定点医疗机构医疗保障基金监管系统的漏洞管理具体要求如下：

a) 应定期进行安全漏洞扫描和评估；
b) 应建立漏洞报告和处理流程，及时响应并处理安全漏洞报告。

9.4 网络安全

定点医疗机构医疗保障基金监管系统的网络和通信安全具体要求如下：

a) 应符合 GB/T 22239 中的不低于等保三级的关于安全通信网络和安全区域边界的规定，并按照 GB/T 39786 中不低于等保三级的网络和通信安全要求执行；
b) 应能够绘制与当前运行情况相符的虚拟化网络拓扑结构图，并应能对虚拟化网络资源、网络拓扑进行实时更新和集中监控和管理；
c) 应采用防火墙、入侵检测系统（IDS）和入侵防御系统（IPS）等网络安全设备；
d) 应对网络通信进行监控和日志记录。

9.5 物理和环境安全

定点医疗机构医疗保障基金监管系统的物理和环境安全具体要求如下：

a) 应符合 GB 50174，GB 50462 的规定，并按照 GB/T 39786，GB/T 22239 中不低于等保三级的物理和环境安全要求执行；
b) 系统服务器和网络设备应设置在安全的物理环境中，如受控机房或数据中心，确保设备的物理安全性；
c) 应采取措施防止未经授权的物理访问，如门禁系统、监控摄像等设备的部署。

9.6 设备和计算安全

应符合GB/T 22239中不低于等保三级的关于安全计算环境的规定，并按照GB/T 39786中不低于等保三级的网络和通信安全要求执行。

10 运维要求

10.1 运维管理

运维管理提供运维工作界面和工具支撑，其功能要求如下：

a) 应支持变更管理和配置一致性检测，且能在失败或发生错误时回滚配置；
b) 应支持维护事件自动提醒，能实时将运维事件通知相关人员；
c) 应支持定期对系统进行健康巡检，能自动生成巡检日志；
d) 应支持自动生成维护报告，能定期提供系统运行情况和资源利用情况的分析报告。

10.2 日常管理

定点医疗机构医疗保障基金监管系统的日常管理要求如下：

a) 应制定系统更新计划和策略，定期更新系统软件版本；
b) 应为用户提供培训和支持服务，提供在线帮助文档和视频教程；
c) 应建立版本管理制度，管理系统各个版本，确保版本控制和一致性。

10.3 应急响应

定点医疗机构医疗保障基金监管系统的应急响应要求如下：

a) 应制定完善的应急响应计划，包括安全事件的报告、响应和恢复流程；
b) 应定期进行安全演练和应急演练，提高系统管理人员和操作人员的应急响应能力。

10.4 安全培训

定点医疗机构医疗保障基金监管系统的安全培训要求如下：

a) 系统管理人员和操作人员应接受安全培训，了解系统安全政策和规范，并学习安全最佳实践；
b) 应定期组织安全培训和意识提升活动，提高全体人员的安全意识和技能水平。