ICS 35.240.80
CCS C 07

团　　体　　标　　准

T/CIIA 046—2024

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

2024－12－20 发布　　2024－12－20 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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国信息协会提出并归口。

本文件起草单位：上海金仕达卫宁软件科技有限公司、上海联众网络信息股份有限公司、东软集团股份有限公司、西南医科大学附属中医医院、中山大学附属第五医院、中国人民解放军陆军军医大学第一附属医院、太极计算机股份有限公司、航天长峰医疗科技(成都)有限公司、山东万天信息科技有限公司、上海唯家保险经纪有限公司、亿保创元(北京)信息科技有限公司、北京新联共创标准化技术有限公司。

本文件主要起草人：赵蒙海、夏春令、田升、钱凯、项峥、刘兵、赵鹏、王昆仑、王亚宗、李峰、程小丽、侯云龙、生训刚、王琳、冒海杨、赵丽丽、张棪、宋宝祥、姜瀚卿、杨海超。

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（以下简称“系统”）的系统架构、功能要求、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 7408.1 日期和时间 信息交换表示法 第1部分：基本原则

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 medical security fund

国家为保障职工的基本医疗，由医疗保险经办机构按国家有关规定，向单位和个人筹集用于职工基本医疗保险的专项基金。

3.2

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。

3.3

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）

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

5 系统架构

定点医疗机构医疗保障基金监管系统支持云系统架构和非云系统架构两种模式，见图1、图2。

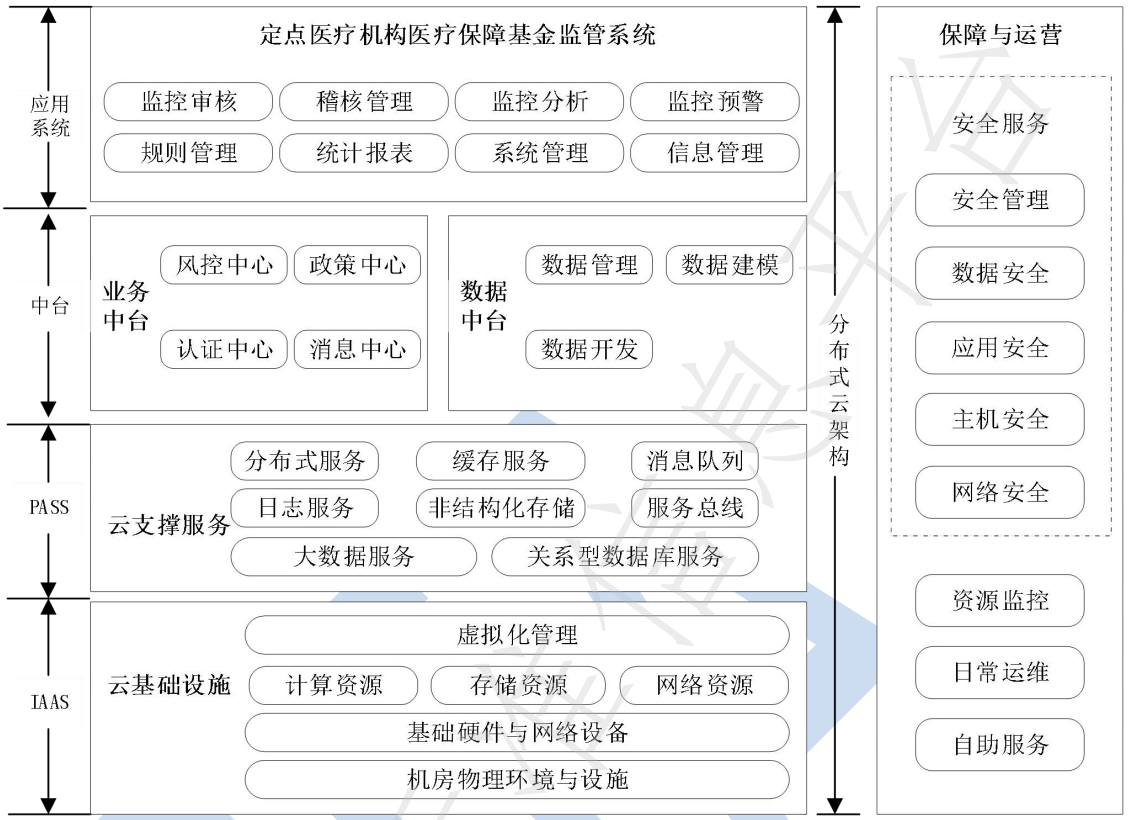

图 1 云系统架构

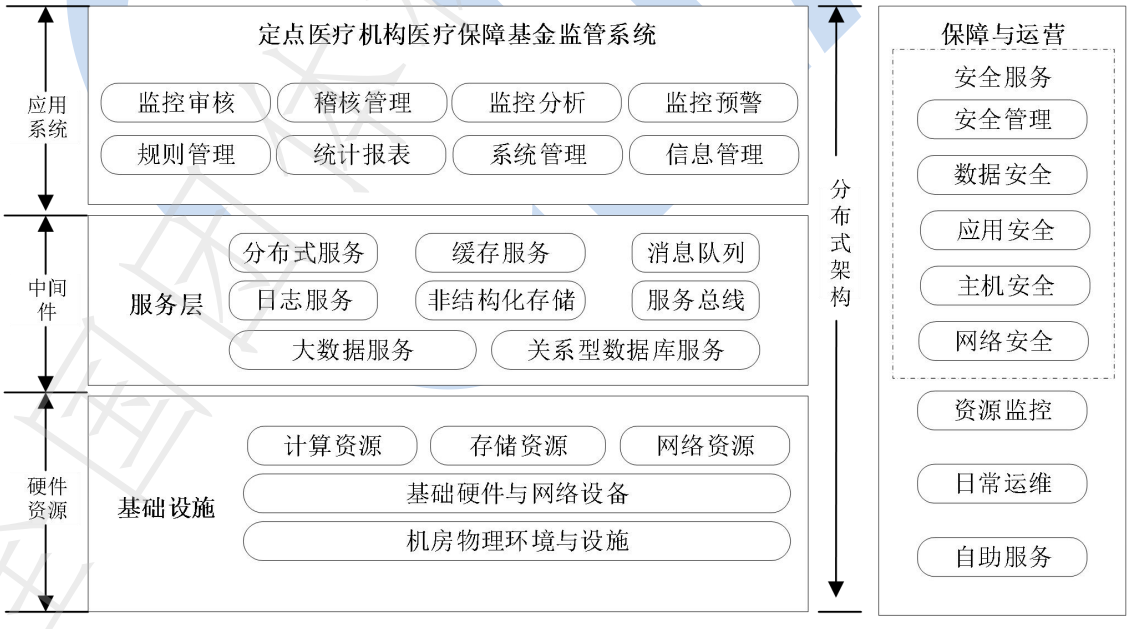

图 2 非云系统架构

6 功能要求

6.1 监控审核

6.1.1 监控审核模块是对医院医务人员的诊疗服务行为进行整体监督，通过多个维度对医保违规行为

进行概览，方便医院管理者浏览和进行违规处理。

6.1.2 监控审核模块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）审核规则的集中汇总；
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，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) 浏览违规数据：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。

6.2 稽核管理

6.2.1 稽核管理模块是医院医保管理人员将系统发现的违规问题或违规线索进行登记，形成稽核任务，根据稽核任务对违规进行现场的查验取证，并对异常行为进行确认，以便医院管理者后续进行违规处理。

6.2.2 稽核管理模块包括但不限于以下功能：

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。

6.3 监控分析

6.3.1 监控分析模块是通过制定医院医保费用相关的分析指标，帮助医院找出影响运营效率的费用因素，从而采取相应的措施进行改进。同时，为医保政策的制定和调整提供重要的数据支持。

6.3.2 监控分析模块包括但不限于以下功能：

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等；
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。

6.4 监控预警

6.4.1 监控预警模块是通过建立医务人员预警提醒，实现诊疗过程与医保结算两个层面的事前、在院、事后的双重全覆盖，优化医保费用使用预警效能、提升医疗行为合规性、保证合理诊疗正常开展。

6.4.2 监控预警模块包括但不限于以下功能：

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，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，医嘱医生对直接违规行为或疑点有异议可提交说明材料；如在患者住院预结算审核中发现临床科室未对违规行为或违规疑点进行整改、未提交说明，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。

6.5 规则管理

6.5.1 规则管理模块面向系统管理人员，主要实现对监管规则内容本身的维护和配置管理。同时，通过对规则执行任务的管理，实现规则的周期性自动化运行。

6.5.2 规则管理模块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：
   1) 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；
   2) 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。

d) 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。

e) 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。

6.6 统计报表

6.6.1 统计报表模块收集和汇总医疗机构监管数据，并根据用户的业务需求创建各种统计维度的报表。

6.6.2 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。

6.7 系统管理

6.7.1 系统管理模块面向系统管理人员，主要实现监管系统的基本项配置和功能管理。

6.7.2 系统管理模块包括但不限于以下功能：

a) 用户管理：
   1) 用户查询：可根据条件查询系统中已存在的用户信息，包括基本信息和登录情况；
   2) 用户新增：支持新增用户信息，包括基本信息和密码，以及权限设置；
   3) 用户编辑：支持对已有用户信息进行修改，包括基本信息和密码的编辑。

b) 角色管理：
   1) 角色查询：支持查询系统中已设置的角色名称和描述；
   2) 角色新增：支持对新增角色信息，包括角色名称和描述；
   3) 角色编辑：支持对已有角色描述进行修改。
c) 模块管理：
   1) 添加模块：支持添加下级或者添加同级模块，以构建系统的功能模块体系；
   2) 修改模块：支持对已有的模块进行相关内容的修改，包括模块的名称、描述等。
d) 权限管理：
   1) 用户角色分配：支持用户分配角色，一个用户可对应多个不同的角色；
   2) 角色模块分配：支持为角色分配系统功能权限，包括模块的访问权限等。
e) 用户权限审核：
   1) 显示申请信息：支持在列表中查看申请访问权限的用户信息和申请的模块信息；
   2) 审核权限：具有审核权限的人员可以对申请信息进行审核，包括同意或拒绝申请。
f) 日志管理：支持生成操作日志明细，包括操作时间、操作人员、操作内容等。

6.8 信息管理

6.8.1 信息管理模块面向系统管理人员，主要实现系统中初始化数据的配置和管理。

6.8.2 信息管理模块包括但不限于以下功能：

a) 药品信息管理：
   1) 应实时监测药品库存情况，包括药品数量、批次、保质期等信息，并支持库存预警和自动补货功能；
   2) 应提供药品信息维护功能，包括录入、编辑、删除药品信息等；
   3) 应记录药品的采购、销售、退货等交易记录，包括交易时间、数量、金额等信息。
b) 医疗机构信息管理：
   1) 应建立医疗机构档案，包括医院、诊所等机构的基本信息、等级、科室设置等；
   2) 应支持对医疗机构的新增、编辑、停用等管理操作。
c) 患者信息管理：
   1) 应建立患者档案，包括个人基本信息、就诊记录、过敏情况、家族病史等；
   2) 应提供就诊预约与管理功能，包括患者在线预约挂号、预约查询、取消预约等操作。
d) 费用信息管理：
   1) 应支持记录和管理患者就诊或服务过程中产生的费用。包括费用项目的名称、数量、单价和总价；
   2) 应支持管理患者支付费用的方式和状态，跟踪费用的支付过程；
   3) 应支持对费用信息进行审核和审批。
e) 医嘱和处方信息管理：
   1) 应支持记录医生对患者的医疗建议或治疗指示，跟踪医嘱的执行情况；
   2) 应支持记录医生开具的处方信息，包括药品名称、剂量、用法、用量等；
   3) 应支持药品库存信息维护，根据医生开具的处方自动扣减相应药品的库存量。

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 7408.1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 7408.1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 7408.1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。

b)　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。

c)　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。

d)　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。

e)　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　接口分类

8.2.1　医保信息平台接口

用于与各级医保部门的医保信息平台（如风控中心、统一认证中心、基础信息中心、用户中心等）进行数据交互，包括但不限于参保人员信息查询、医保待遇结算信息上传、医保目录信息同步等功能接口。

8.2.2 医院信息系统（HIS）接口

8.2.2.1 实现与定点医疗机构内部的医院信息系统对接，获取医疗服务过程中的各类数据，如患者诊疗记录、医嘱信息、费用明细等。

8.2.2.2 接口宜考虑不同医院信息系统的差异性，具备良好的兼容性和可扩展性，以适应各类医疗机构的接入需求。

8.2.3 其他外部系统接口

应根据实际业务需求，提供与其他外部系统（如药品监管系统、医疗设备管理系统等）进行数据交互的接口，明确数据交换的内容、格式和方式，以实现数据交换、信息传递或业务流程的协同。

8.3 技术要求

8.3.1 通信协议

8.3.1.1 应采用基于 HTTP/HTTPS 的 RESTful 架构风格进行接口设计，实现轻量级、易于理解和使用的接口通信。

8.3.1.2 对于数据传输实时性要求较高的场景，宜采用 WebSocket 等全双工通信协议，确保数据能够及时、准确地传输。

8.3.2 数据格式

8.3.2.1 接口数据传输宜采用 JSON 格式，以保证数据的简洁性、可读性和跨平台兼容性。

8.3.2.2 对于特殊业务场景或对数据结构有严格要求的接口，可根据实际情况选择使用 XML 格式，并在接口文档中明确说明。

8.3.3 接口安全

8.3.3.1 宜采用 SSL/TLS 协议等数据加密技术对 HTTP 通信进行加密处理。

8.3.3.2 应实施身份认证机制，在接口调用方和被调用方之间进行身份验证。可采用基于 Token 的认证方式或数字证书认证等方式，具体认证方式应根据系统的安全级别和业务需求确定。

8.3.3.3 应对接口访问进行授权管理，根据不同的业务功能和数据权限，为接口调用方分配相应的访问权限。

8.3.4 调用方式

8.3.4.1 基本要求

接口调用基本要求如下：

a) 应使用 HTTP 或 HTTPS 协议进行接口调用，确保数据传输安全可靠；
b) 应根据操作类型选择合适的 HTTP 请求方法，如 GET、POST、PUT、DELETE 等；
c) 接口 URL 应明确主机地址、端口号（可选）、接口路径等部分；
d) 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。

8.3.4.2 参数传递

接口参数传递要求如下：

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。

8.3.4.3 返回数据

接口返回数据要求如下：

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附录 A。

9 安全要求

9.1 访问控制

系统的访问控制具体要求如下：

a) 应采用用户身份验证机制，包括用户名和口令验证，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

系统的数据保护具体要求如下：

a) 应符合 GB/T 22239 中相应等级的关于安全审计、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 中相应等级的应用和数据安全规定执行，根据医院级别不同：
   1) 三甲医院应符合 GB/T 22239 中不低于等保三级的规定，并按照 GB/T 39786 中不低于第三级密码应用基本要求执行；
   2) 二甲医院及规模较大的综合医院应符合 GB/T 22239 中不低于等保二级的规定，并按照 GB/T 39786 中不低于第二级密码应用基本要求执行；
   3) 基层诊所等小型医疗机构应符合 GB/T 22239 中不低于等保一级的规定，并按照 GB/T 39786 中不低于第三级密码应用基本要求执行。
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。对核心业务数据每日全量备份，对日志数据等进行增量备份，备份数据存储于异地灾备中心；
d) 应根据不同级别医院系统数据增长趋势预设容量并保障扩展性；
e) 应明确违规存证记录管理策略。三甲医院存证不少于 5 年，二甲医院不少于 3 年，基层诊所不少于 1 年。
f) 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 网络安全

系统的网络和通信安全具体要求如下：

a) 应符合 GB/T 22239 中相应等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 中相应等级的网络和通信安全要求执行，根据医院级别不同：
   1) 三甲医院应符合 GB/T 22239 中不低于等保三级的规定，并按照 GB/T 39786 中不低于第三级密码应用基本要求执行；
   2) 二甲医院及规模较大的综合医院应符合 GB/T 22239 中不低于等保二级的规定，并按照 GB/T 39786 中不低于第二级密码应用基本要求执行；
   3) 基层诊所等小型医疗机构应符合 GB/T 22239 中不低于等保一级的规定，并按照 GB/T 39786 中不低于第三级密码应用基本要求执行。
b) 应能绘制与当前运行情况相符的虚拟化网络拓扑结构图，并对虚拟化网络资源、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）等网络安全技术，构建多层次的网络安全防护体系；
d) 应对网络通信进行监控和日志记录。

9.4 物理和环境安全

系统的物理和环境安全具体要求如下：

a) 应符合 GB 50174、GB 50462 和 GB/T 22239 的规定，并按照 GB/T 39786 中相应等级的物理和环境安全规定执行，根据医院级别不同：
   1) 三甲医院应符合 GB/T 22239 中不低于等保三级的规定，并按照 GB/T 39786 中不低于第三级密码应用基本要求执行；
   2) 二甲医院及规模较大的综合医院应符合 GB/T 22239 中不低于等保二级的规定，并按照 GB/T 39786 中不低于第二级密码应用基本要求执行；

3) 基层诊所等小型医疗机构应符合GB/T 22239中不低于等保一级的规定，并按照GB/T 39786中不低于第三级密码应用基本要求执行。

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。

9.5 设备和计算安全

应符合GB/T 22239中相应等级的关于设备和计算安全的规定，并按照GB/T 39786中相应等级的设备和计算安全要求执行，根据医院级别不同：

a) 三甲医院应符合 GB/T 22239 中不低于等保三级的规定，并按照 GB/T 39786 中不低于第三级密码应用基本要求执行；

b) 二甲医院及规模较大的综合医院应符合 GB/T 22239 中不低于等保二级的规定，并按照 GB/T 39786 中不低于第二级密码应用基本要求执行；

c) 基层诊所等小型医疗机构应符合 GB/T 22239 中不低于等保一级的规定，并按照 GB/T 39786 中不低于第三级密码应用基本要求执行。

10 运维要求

10.1 运维管理

10.1.1 应安排专人负责系统运维工作，接收系统配置变更的相关信息，并在内部建立配置变更审核机制，确保变更管理和配置一致性检测流程得到有效执行。配置失败或发生错误时，及时启动回滚配置操作，同时详细记录整个过程以便追溯和分析。

10.1.2 应支持维护事件自动提醒，可通过多种方式（如短信、系统弹窗、邮件等）实时将运维事件通知相关人员。

10.1.3 应定期对系统进行健康巡检，生成巡检日志并保存。

10.1.4 应组织相关技术人员和业务骨干定期对维护报告进行研读和分析。结合自身业务发展需求和实际使用体验，提出优化建议和功能改进需求。

10.2 日常管理

10.2.1 应定期更新系统版本，在更新前应进行充分的测试与评估，确保更新不会对现有业务造成影响。

10.2.2 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，定期收集用户反馈，不断优化培训内容与方式，提升用户对系统的操作熟练度与问题解决能力。

10.3 应急响应

10.3.1 应制定应急响应计划，明确安全事件报告流程，包括报告时间、方式及事件详情描述要求，同时确定各部门在应急中的职责分工与协同机制。

10.3.2 应定期进行安全演练和应急演练，涵盖网络攻击等常见安全事件类型，模拟真实场景检验各部门人员对应急计划熟悉与执行能力，演练后召开总结评估会，深入剖析应急响应流程、部门协作及技术手段有效性等方面问题并制定改进措施完善计划与能力。

10.4 安全培训

10.4.1 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。

10.4.2 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。

附录 A
（资料性）
接口调用返回错误定义类型

接口调用返回错误定义类型见表A.1。

表 A.1 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

参 考 文 献

[1] XJ-A01-2019 医疗保障信息平台云计算平台规范
[2] XJ-B01-2019 医疗保障信息平台应用系统技术架构规范
[3] XJ-C01.1-2019 医疗保障信息平台用户界面规范 第1部分：PC端用户界面规范
[4] 医疗保障基金使用监督管理条例（国务院令第735号）
[5] 国务院办公厅关于推进医疗保障基金监管制度体系改革的指导意见（国办发〔2020〕20号）
[6] 国务院办公厅关于加强医疗保障基金使用常态化监管的实施意见(国办发〔2023〕17号)