ICS 35.240.80
C 07

YB

医保网络安全和信息化标准

XJ-A01-2019

医疗保障信息平台
云计算平台规范

2019-09-06 发布　　2019-09-06 实施

国家医疗保障局网络安全和信息化领导小组办公室　发布

目次

前言

本标准按照 GB/T 1.1-2009 给出的规则起草。

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这些专利的责任。

本标准由国家医疗保障局规划财务和法规司提出并归口。

本标准起草单位：国家医疗保障局规划财务和法规司。

医疗保障信息平台 云计算平台规范

1 范围

本规范规定医疗保障信息平台云计算平台的功能、性能、安全、保障和运维等方面的要求。

本规范适用于医疗保障信息平台云计算平台的建设。

2 规范性引用文件

下列文件对于本文件的应用事必不可少的。凡注日期的文件，仅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 50174-2017 数据中心设计规范

GB/T 22239-2019 信息安全技术网络安全等级保护基本要求

YB XJ-B01-2019 医疗保障信息平台应用系统技术架构规范

3 术语和定义

3.1

计算资源 computing resource

云计算平台提供的服务器、虚拟机等资源。

3.2

存储资源 storage resource

云计算平台提供的存储空间、数据备份、数据灾备等资源。

3.3

网络资源 network resource

云计算平台提供的网络传输、虚拟网络、IP 地址、虚拟网络等资源。

3.4

资源池 resource pooling

一组物理资源或一组虚拟资源的集合，可以从池中获取资源、也可将资源回收到池中。资源包括物理机、虚拟机、虚拟网络设备、物理网络设和IP地址等。

3.5

租户 tenant

使用云计算平台的用户，每个用户能按需使用资源，能够对云计算平台资源进行个性化配置且不影响其他用户的使用。

4 缩略语

下列英文缩略语适用于本文件。

HSAF 医疗保障应用框架（Healthcare Security Application Framework）
IaaS 基础设施即服务（Infrastructure-as-a-Service）
PaaS 平台即服务（Platform-as-a-Service）
SaaS 软件即服务（Software-as-a-Service）
CPU 中央处理器（Central Processing Unit）
QoS 服务质量（Quality of Service）
I/O 输入/输出（Input/Output）
Web 全球广域网（World Wide Web）
ISV 独立软件开发商（Independent Software Vendors）
API 应用程序编程接口(Application Programming Interface)
SDK 软件开发工具包（Software Development Kit）
ACL 访问控制列表（Access Control Lists）
DDoS 分布式拒绝服务攻击(Distributed Denial of Service)
SQL 结构化查询语言(Structured Query Language)
TCP 传输控制协议（Transmission Control Protocol）
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)
MQTT 消息队列遥测传输协议(Message Queuing Telemetry Transport)
UTF8 8位统一码转换格式（8-bit Unicode Transformation Format）
GBK 汉字内码扩展规范
ASCII 美国信息交换标准代码(American Standard Code for Information Interchange)
JSON Java脚本对象简谱(JavaScript Object Notation)
VPC 虚拟私有云（Virtual Private Cloud）

5 医保云计算平台总体架构

5.1 总体原则与要求

由于医疗保障业务的重要性和复杂性，原则上建议地方自建数据中心，如采用政务云，须保证专有、独享原则，应对政务云提出规划独立设备、专有网络、专属安全、专属 PaaS 资源等，同时上述资源须能支撑医保业务中台的技术要求。

5.2 总体技术架构

医疗保障云计算平台采用分布式云架构,在私有化的云基础设施层上,提供大数据服务、关系型数据库服务、日志服务、存储服务、服务网关、分布式服务、缓存服务、消息队列服务支撑，为上层的 HSAF 框架（详见 XJ-B01-2019 2.2 定义）及应用系统提供标准化支撑。HSAF 适配框架适配分布式微服务、分布式消息队列、分布式缓存、分布式数据库中间件、分布式非结构存储等，详见《医疗保障信息平台应用系统技术架构规范》。

各省应依据医保云计算平台总体架构，建立省级多数据中心，并行运行，互为容灾，来进行生产维护、日常操作等工作。

医保云计算平台总体技术架构见图 1。

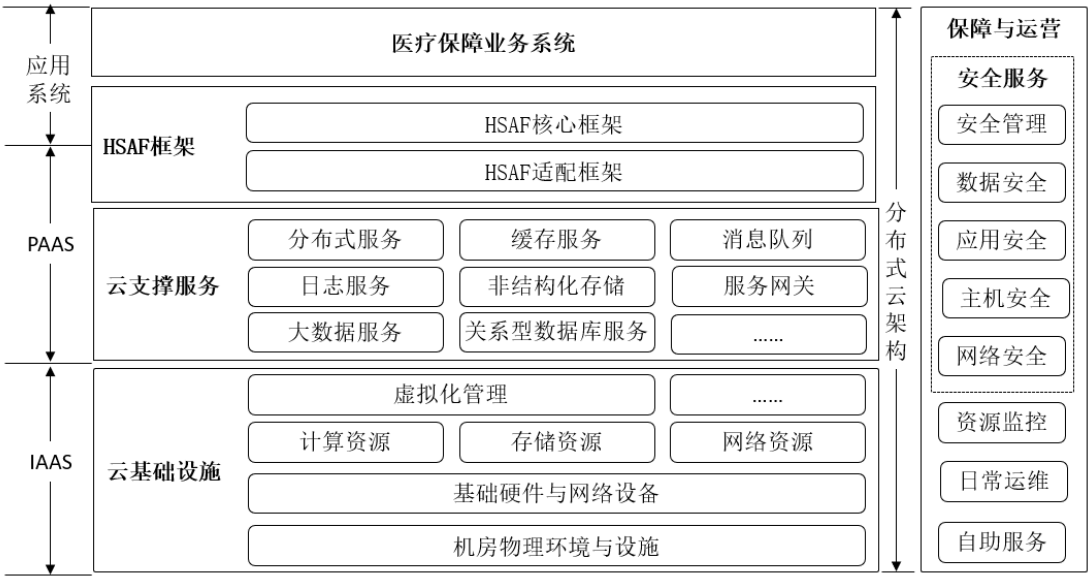

图 1 总体技术架构

5.3 云支撑服务技术兼容性要求

云支撑服务技术兼容性要求如下：

a) 应满足 HSAF 框架的适配实现技术，包括分布式技术和数据库产品等，详见《医疗保障信息平台应用系统技术架构规范》8.2 和 8.3。

b) 各地医保系统做技术合规选型时，如采用 HSAF 框架预设适配实现技术之外的技术，应做相应适配、开发工作。

c) 国家下发的 HSAF 框架版本验证了开源产品的兼容性，各地医保采用开源产品，其稳定性、可管理性、性能等应由承建商保证。

d) 各地采用的开源产品不满足云规范要求的特性、功能、能力，应由承建商开发实现。

e) 技术选型（尤其是数据库选型）应考虑国家对国产化、自主可控的要求。

5.4 云基础设施层和云支撑服务层总体非功能性要求

云基础设施层和云支撑服务层的总体非功能性要求如下：

a) 应保证云基础设施层和云支撑服务层 7*24 小时的连续性；

b) 应保证云基础设施层和云支撑服务层可用性达到 99.9%；

c) 应保证云基础设施层和云支撑服务层存储数据的可靠性达到 99.9999%。

6 云基础设施层功能和性能

6.1 基础硬件设施要求

基础硬件设施是指机房等基础设施以及计算、存储、网络等硬件设备，是云计算平台的物理基础。

云计算平台硬件设备应使用安全可控、体系架构开放的计算、存储、网络等硬件设备进行构建，保障安全性、可用性和可靠性。应使用专有的机柜和配电，应跟机房的其它非业务相关环境实现网络物理隔离。机房在选址、建筑结构、供电、制冷、消防、布线、物理访问控制、防盗防破坏等方面应符合 GB 50174-2017 中第 8 章（电气要求）、第 10 章（网络与布

线）、第 11 章（智能化系统）的要求。

6.2 计算资源

计算虚拟化技术能够利用虚拟化软件从计算资源池中虚拟出一台或多台虚拟机。虚拟化软件的功能要求如下：

a） 应支持多虚拟机管理与配置；
b） 应支持不同虚拟机之间资源逻辑隔离；
c） 应支持对 CPU、内存等资源进行 QoS 配置；
d） 应支持 CPU、内存使用的上限和下限设置；
e） 应支持虚拟机 CPU、内存的配置动态调整；
f） 应支持计算资源池化，提供可动态调整的 CPU、内存、I/O 设备等资源。

6.3 存储资源

6.3.1 存储资源管理

存储资源管理负责存储系统资源的管理，其功能要求如下：

a） 应支持按存储资源类型实现资源池的分类管理和调度。
b） 应支持存储资源灵活调配的功能；
c） 应支持通过精简配置等功能提升存储资源利用率；
d） 应支持多种存储系统的统一管理。

6.3.2 存储系统

存储系统的功能要求如下：

a） 应支持高可扩展性，支持数据的存储和读写；
b） 应支持故障自动侦测、故障隔离和数据迁移，避免单点故障风险；
c） 应具备可靠的数据存储保护能力；
d） 应支持存储系统在线扩容和自动数据平衡；
e） 应支持集中式存储和分布式存储；
f） 应支持硬盘、存储服务器、磁盘阵列等存储资源；
g） 应支持存储容量按需扩容；
h） 应支持屏蔽相同架构类型下不同硬件的实现差异；
i） 应为上层应用提供存储资源的抽象，包括但不限于块存储、文件存储和对象存储等；
j） 应提供块存储接口、文件存储接口和对象存储接口等存储系统与外部的接口，支持高速可靠的数据传输。

6.4 网络资源

6.4.1 概述

数据中心应进行网络区域划分。网络区域应划分为提供核心业务服务的核心业务区、提供互联网服务的公共服务区；互联网访问、各个区域之间以及多数据中心之间，应采用双链路网络保障通讯的高可用性。

6.4.2 网络资源管理

网络资源管理将物理和虚拟网络资源形成资源池进行统一管理调度。网络资源管理的功能要求如下：

a) 应采取冗余架构等措施，避免网络资源管理节点的单点故障；
b) 支持对不同厂商网络设备的管理和配置自动下发，包括子网、网关、路由等参数的配置。

6.4.3 网络虚拟化

利用网络虚拟化可在一个物理网络上模拟出多个虚拟网络。网络虚拟化包括网卡的虚拟化，物理网络设备的虚拟化，租户网络的虚拟化，以及网络功能虚拟化。网络虚拟化的功能要求如下：

a) 应支持将物理网络设备虚拟化为逻辑网络设备使用；
b) 应支持挂载和卸载虚拟机网卡；
c) 应支持端口镜像，满足远程运维和故障分析需求；
d) 应支持虚拟机和物理网卡直通功能，提升虚拟机网络性能；
e) 应支持通过隧道封装技术为租户构建独立隔离的虚拟网络；
f) 应支持为不同的租户构建独立的虚拟网络，租户间的网络隔离；
g) 应支持根据业务需求实现同一租户或不同租户 VPC 之间的互通；
h) 应支持虚拟网络和物理网络之间的三层交换。

6.5 虚拟化管理

虚拟化管理是指云服务提供者向云服务使用者提供面向操作系统的计算服务。虚拟化管理的功能要求如下：

a) 应具备虚拟机全生命周期管理功能，支持对虚拟机进行创建、删除、回收、暂停、恢复、关闭、重启等操作；
b) 应支持不同类型的操作系统和存储设备；
c) 应支持创建自定义 CPU、内存、网络、磁盘等属性的虚拟机；
d) 应支持对运行或停止状态的虚拟机生成快照，并提供快照回滚功能；
e) 应支持计算能力的垂直伸缩，如 CPU 和内存的升级与降级、磁盘和网卡的增加与减少等；
f) 应支持计算能力的水平伸缩，如创建、删除虚拟机实例等；
g) 应支持自定义网络配置；
h) 应支持故障场景下的虚拟机恢复；
i) 应应支持将虚拟机在运行情况下迁移至其他宿主机。

7 云支撑服务层功能和性能

7.1 分布式服务

分布式服务是一个应用托管和微服务管理的 PaaS 平台，提供应用开发、部署、监控、运维等全栈式解决方案，支持微服务运行环境。分布式服务功能要求如下：

a) 应提供 rpc、restful 等通用协议进行服务间通信；
b) 应提供自动化的服务注册，服务自动发现，服务检查能力；
c) 应支持对服务进行全生命周期管理，支持应用的发布，部署、启停、升级、回滚等全生命周期管理能力，并提供 Web 界面形式的运维管控平台；
d) 应支持应用服务线性扩展能力，支持 Web 界面应用自动扩缩容；
e) 应提供应用实时日志的 Web 界面可视化展示，实时跟踪日志输出并展示，并提供大批量日志存储备份功能；

f) 应提供配置中心能力，可以对配置进行管理，版本控制，下发，配置热更新等；
g) 应提供应用层基础指标的监控，固定时间段内请求量监控能力；
h) 应提供分布式事务功能；
i) 应提供服务认证授权能力，支持熔断容错机制，支持上下文信息传递；
j) 应提供服务管理能力，支持集群和命名空间能力，支持命名空间隔离，支持服务分组；
k) 应提供限流规则的配置，允许指定服务提供者针对某些消费者的，接口级、方法级的单位时间最多处理服务量；
l) 应支持对服务调用链的追踪，支撑梳理调用依赖、分系统瓶颈、估算容量、定位异常等；
m) 应支持对服务实例进行选择，完成客户端和服务端负载均衡；
n) 应支持应用依赖分析，依赖拓扑图展示能力；
o) 应提供完整的多用户隔离机制，保障用户数据的私密性，同时应满足多 ISV 协同开发的问题；
p) 应具备完善的主子账号体系,能够实现同一个主账号将自己的资源按需分配给多个子账号；
q) 应提供角色、权限控制和资源组定义，精细的控制不同子账号之前的操作权限、资源权限；
r) 应支持应用的本地调用堆栈收集和统计，能统计出关键函数的调用时长；
s) 应支持业务全息排查，可通过业务 ID 关联具体调用链查询，对程序故障进行诊断；
t) 应支持内存分析功能，可通过界面动态执行内存 Dump，收集，分析，展示功能，能分析内存的对象使用情况。

7.2 缓存服务

缓存服务基于高可用架构，满足高读写性能及快速数据访问需求的分布式内存数据库。缓存服务的功能要求如下：

a) 应支持高可用集群模式，性能可线性提升；
b) 应支持内存和硬盘的持久化存储方式；
c) 应支持基于事件通知机制，解耦消息发布者和消息订阅者之间的耦合，实现消息发布及订阅 (PUB/SUB)功能，提供分钟级别的监控功能；
d) 应支持虚拟网络，可支持指定虚拟网络创建内存数据库实例；
e) 应支持在线平滑升降级，计算能力、内存容量和总 I/O 带宽同步线性扩容；
f) 应兼容主流协议，如 Redis；
g) 应有完善用户账号控制策略和白名单策略，提高数据库集群的安全性。

7.3 消息队列服务

消息队列是构建分布式应用的基础设施，消息队列用于实现松耦合架构设计，以提高系统可用性以及可扩展性。消息队列服务功能要求如下：

a) 应提供分布式消息队列服务；
b) 应支持发布订阅模型；
c) 在单个消息生产者情况下，应支持顺序消息，包括消息的顺序发送与顺序接收；
d) 应提供 Web 管理界面及管理命令集；
e) 应提供消息回溯消费功能；
f) 应提供监控报警功能；

g) 应提供管理类 API 和管理控制台；
h) 应提供日志记录功能；
i) 应提供 JAVA、PHP、Python 等 SDK 接入，支持 TCP、HTTP、MQTT 等多种协议接入；
j) 应具备完善的多用户隔离机制，保障用户数据的私密性；
k) 应支持主-主账号授权及主-子账号授权模式；
l) 应具备多层次安全防护和防 DDoS 攻击能力，支持跨地域的安全消息服务；
m) 应能为每个消息服务提供单独命名空间，保证客户间数据严格隔离；
n) 应提供优先级队列功能；
o) 应提供对消息加密功能；
p) 应支持队列数量及队列存储容量的扩展，应支持亿级消息收发、推送、堆积，容量不设上限。

7.4 日志服务

日志服务提供分布式日志采集、日志存储、日志内容搜索、统计分析等服务。日志服务的要求如下：

a) 应支持大规模接入各种实时日志数据；
b) 应支持与各种实时计算及服务对接，并提供完整的进度监控，报警等功能；
c) 应支持日志投递功能，并将日志数据投递至存储类服务，过程支持压缩、自定义分区 以及行列等各种存储格式；
d) 应支持实时检索日志数据，提供关键词、模糊、上下文、范围、SQL 聚合等丰富查询手段，提供仪表盘及报警功能；
e) 应支持多租户隔离，访问控制，日志审计。

7.5 非结构化存储

非结构化存储是指为云服务使用者提供非结构化数据存储的服务，存储容量和处理能力能弹性扩展，适合存放任意类型的文件。在云环境下通常用对象存储的方式提供服务。

对象存储服务以数据标记为主要的文件组织方式，提供完全扁平化的存储服务。对象存储服务的功能要求如下：

a) 应提供基于多租户的身份认证和数据隔离等存储管理功能；
b) 应支持通过冗余副本、集群等方式保障高可靠性；
c) 应支持低延时、高并发的数据访问；
d) 应支持存储容量的在线扩展；
e) 应支持对象存储用户的配额的设置和检查，保证使用容量达到配额后不能继续占用更多存储空间。

7.6 大数据服务

7.6.1 概述

大数据服务提供按需部署大数据处理服务以实现医保机构的大数据处理需求。

7.6.2 大数据离线计算能力

大数据服务应具备大数据离线计算能力，具体要求如下：

a) 应提供多租户协作和 ACL 权限控制功能，支持敏感数据访问控制；应实时记录敏感数据访问行为以支持定期的安全审计，严控内部数据安全风险；
b) 应支持实时数据接入，包括 Flume、Kafka 数据接入，应支持包含结构化、半结构

化、非结构化的异构数据实时接入；

c) 应支持离线数据导入，包括 MySQL、Postgre、Oracle 等主流关系数据库高效导入，包括文本类日志数据离线导入；

d) 应支持页面自助化配置数据采集方式，包括数据实时采集与周期性采集；

e) 应提供多类型存储支持，包括分布式文件存储、对象存储、NoSQL 从 GB 到 PB 量级的存储；

f) 应支持 MapReduce、Hive 批处理计算作业，能支撑数仓建设中的数据清洗、转换、汇集、主题提取等数据处理需求；

g) 应提供多维分析引擎，能支持任意维度组合分析、实时下钻分析；

h) 应支持图计算处理框架，实现复杂的数据挖掘算法和图计算算法。

7.6.3 大数据实时分析能力

大数据服务应具备大数据实时分析能力，具体要求如下：

a) 应提供分布式实时计算能力，支持在内存中对数据集进行快速多次迭代；

b) 应提供多维实时分析作业引擎，支持任意维度的灵活自由查询分析服务，支持实时数据写入并提供实时查询分析服务能力，覆盖实时要求极高的流式作业场景；

c) 应支持符合 SQL2003 标准的查询语法和 OLAP 分析聚合函数，提供灵活的混合分析能力。

7.6.4 大数据治理开发能力

大数据服务应具备大数据治理开发能力，具体要求如下：

a) 应提供数据集成能力，包括数据采集、数据同步、数据交换和数据转换等能力；

b) 应提供大数据治理的能力，能通过数据校验规则、监控规则、形成数据质量信息评估等；

c) 应提供对接入的所有数据源的统一标准化管理，能记录每个数据源所有字段、类型、长度信息，能记录每个数据源的数据量、数据增长情况、空间使用率；

d) 应支持数据流转的全流程可视化血缘跟踪溯源，包括库表数据和任务流关系分析、数据来源及流向分析；

e) 应提供高可靠分布式的任务调度能力，支持轮询分布式执行代理和指定特定代理节点执行任务；

f) 应支持丰富的调度策略，包括分钟、小时、天、月级周期或非周期的任务执行策略；

g) 应支持监控报警，包括存储监控、调度任务监控，能对监控提供短信报警。

7.6.5 大数据智能报表能力

大数据服务应具备智能报表能力，具体要求如下：

a) 应提供报表系统，支持添加多个数据源连接、创建数据集、可拖拽制作报表；

b) 应提供有丰富的可视化模板；

c) 应提供丰富的组件；

d) 应提供 Web 表格编辑能力；

e) 应支持多租户协同。

7.6.6 大数据可视化大屏能力

大数据服务应具备可视化大屏能力，具体要求如下：

a) 应支持数据库类、API 类、文件类等数据的接入、配置；

b) 应支持绘制包括海量数据的地理轨迹、地理飞线、热力分布、地域区块、3D 地图、3D 地球，应支持地理数据的多层叠加；
c) 应支持第三方图表库对接，支持原生组件式的拖拽布局与数据接入；
d) 应支持设置发布和访问密码；
e) 应提供可视化大屏发布预览功能。

7.7 关系型数据库服务

7.7.1 概述

关系型数据库服务包含集中式关系型数据库服务和分布式关系型数据库服务。

7.7.2 集中式关系型数据库服务

集中式关系型数据库服务的功能要求如下：
a) 应基于集群及负载均衡等技术提供高可用性；
b) 应具备纵向和横向的扩展能力；
c) 应支持多种技术方案的读写分离；
d) 应支持数据库集群的节点在线扩容和升级；
e) 应提供数据同步功能，能支持实时、离线方式进行数据迁移；
f) 应支持基于多租户的数据存储和数据隔离；
g) 应具备线程池能力；
h) 应具备数据审计能力；
i) 应具备数据库连接加密和透明加密能力；
j) 应记录数据库操作日志；
k) 应支持权限管控和角色划分，例如避免普通用户误操作、删除关键元数据等；
l) 应提供性能分析功能，能输出诊断报告；
m) 应支持基于云多租户的方式分配管理数据库实例；
n) 应具备数据库的监控和报警能力。

7.7.3 分布式关系型数据库服务

分布式关系型数据库服务支持多节点的关系型数据库处理,其应在具备集中式关系型数据能力基础上，还应满足要求如下：
a) 应支持跨数据库节点的数据操作，并保证数据的一致性；
b) 应支持数据库的横向扩容和分库分表；
c) 应支持数据库算法跨数据库节点进行数据处理，保证数据处理的准确性；
d) 应支持多节点数据库的统一监控运维；
e) 应支持某些数据库高级特性，包括但不限于事务、联机查询（JOIN）、索引、全局唯一字段、分区表、预处理协议、聚合函数等；
f) 应支持多种字符集，包括但不限于 UTF8，GBK，LATIN，ASCII，BIG5 等；
g) 应支持多种数据类型，包括但不限于数字，字符，日期，空间类型，JSON 等；
h) 应支持与关系型数据库混合部署，提高资源利用率。

7.8 服务网关

服务网关功能要求如下：
a) 应提供 API 服务接口的完整生命周期管理功能，包括注册、发布、授权、审核、监控等；

b) 应支持 HTTP/HTTPS、Dubbo 通讯协议（Dubbo 与 HTTP 协议的互转能力）等常用协议服务互联；
c) 应支持包括加密、鉴权、流量控制保护、黑白名单等访问控制的服务安全调用；
d) 应采用无状态 API 服务的集群结构；
e) 应采用多级缓存系统；
f) 应支持横向扩展，可满足超大规模性能需求，提供高可靠性，保障 7*24 小时不间断服务；
g) 应支持在大型复杂的网络安全隔离环境下，实现应用服务的注册、发布和调用。

8 安全要求

8.1 概述

应满足 GB/T 22239-2019 网络安全等级保护基本要求中的第三级安全要求，还应满足网络安全、主机安全、应用安全、数据安全和安全管理方面的其他要求。

8.2 网络安全

网络安全方面的具体要求如下：
a) 应支持 DDos 防护，秒级响应攻击，本地防护能力能防护不低于 20Gbps 峰值攻击流量，互联网侧防护宜采用云防护方式提供可扩展的防护能力；
b) 应支持对流量进行深度包分析，能实时检测各种攻击和异常行为，并支持进行阻断；
c) 应支持检测内部的恶意主机对外发起的攻击行为，能发现和定位内部已经被控制的云服务器。

8.3 主机安全

主机安全方面的具体要求如下：
a) 应支持账户安全检测、弱口令检查、配置项安全检测；
b) 应支持云服务器漏洞检查和一键修复；
c) 应支持脚本后门查杀；
d) 应支持对暴力破解的实时检测和拦截；
e) 应支持对疑似非常用登录行为进行告警；
f) 应支持检测反弹 shell、java 进程调用 cmd、bash 异常文件下载等进程异常行为。

8.4 应用安全

应用安全方面的具体要求如下：
a) 应支持防护 SQL 注入、XSS 跨站脚本、文件上传、敏感信息泄露、常见 CMS 漏洞、代码执行注入、脚本后门攻击等；
b) 应支持对大量慢速请求攻击的防护，能根据统计响应码、URL 请求分布、异常 Referer 及 User-Agent 特征识别进行防护；
c) 应提供针对 CC 攻击的防护能力，支持针对域名和 URL 的访问频次控制规则，能够对满足条件的 IP/SESSION 进行访问频率限制或者封禁；
d) 应支持 HTTPS 流量防护。

8.5 数据安全

数据安全方面的具体要求如下：

a) 应通过数据加密、脱敏等策略，确保云内数据不被泄露。
b) 应支持基于国家密码管理局检测认证的硬件密码机提供密码服务，支持算法应包括对称密码算法（支持 SM1、SM4、DES、3DES、AES）、非对称密码算法（支持 SM2、RSA（1024-2048））、摘要算法（支持 SM3、SHA1、SHA256、SHA384）；
c) 应支持对敏感数据的自动识别，能通过数据漂白、动态掩码等方式进行脱敏处理；
d) 应支持数据库应用用户关联审计；
e) 应具备风险状况、运行状况、性能状况、语句分布的实时监控能力。

8.6 安全管理

安全管理方面的具体要求如下：
a) 应具备安全态势可视化能力，能集中总览如紧急事件数量、今日攻击、今日弱点、安全攻击趋势、最新威胁分析展示、最新情况展示等安全态势；
b) 应具备安全告警功能，告警字段需包含：告警名称、告警描述、触发告警规则，触发告警数据，告警目标/源 IP、告警级别，告警时间等；
c) 应支持检测 Web 漏洞利用、攻击扫描、webshell 等安全事件。

9 保障要求

9.1 保障机制

医保云计算平台的建设和使用过程中应制定保障机制，明确总体目标、范围、工作原则和制度要求。保障机制的具体要求如下：
a) 应制定由医保云计算平台管理制度、资源分配管理规范、运维管理手册、应急处理预案等组成的全面的管理制度体系；
b) 应定期对制度体系进行论证和评审，对存在不足或需要改进的制度进行修订。

9.2 保障团队

医保云计算平台的数据中有个人隐私、支付交易类等具有高度敏感性质的专有数据，因此各级医保云计算平台应建立专业的组织机构保障，组建专有的建设及运维保障团队，并设定相关岗位，具体要求如下：
a) 应明确各项目建设和运维团队和岗位职责；
b) 应对各类项目参与人员应进行安全意识教育和岗位技能培训；
c) 应加强各类项目参与人员和团队之间的沟通和协作。

9.3 保障措施

应提供完善的保障措施，具体包括：
a) 应提供技术保障措施，包括：
   1) 服务台及管理工具；
   2) 资源管理工具；
   3) 技术服务管理工具；
   4) 运维服务管理工具；
b) 应提供辅助管理保障措施，包括：
   1) 知识库管理；
   2) 备品备件服务；
   3) 灾备管理服务；

c） 应提供应急响应保障措施，包含应急预案、监测与预警、应急处置、评估与改进等。

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，且能在失败或者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） 应支持定期对云计算平台的资源和应用系统进行健康巡检，能自动生成巡检日志；

d） 应支持自动生成维护报告，能定期提供平台运行情况和资源利用情况的分析报告。

10.2 资源监控

资源监控的功能要求如下：

a） 应提供信息采集功能，能实时采集云计算平台包括硬件、服务器等各类资源及服务的状态信息；

b） 应提供数据分析功能，能对采集信息进行综合分析、准确诊断和动态展示；

c） 应提供资源池监控功能，能对各类资源运行状态进行实时监控；

d） 应提供其他监控平台的接入接口。

10.3 自助服务

自助服务主要向云服务使用者提供可自由调配资源和使用云服务的功能，自助服务的功能要求如下：

a） 应支持自助完成资源的申请、使用、配置、修改、删除；

b） 应支持自助查看申请资源的使用情况、性能状况、审批流程、操作日志等；

c） 应支持对计算、存储、网络等资源的自助调度。