附件：

一、原 5 月 24 日本项目更正公告附件中：

上海市松江区方塔中医医院智慧医院建设招标项目的潜在投标人应在上海政府采购网获取招标文件，并于 2026-06-26 10:00:00（北京时间）前递交投标文件。

现更正为：

上海市松江区方塔中医医院智慧医院建设招标项目的潜在投标人应在上海政府采购网获取招标文件，并于 2026-07-13 10:00:00（北京时间）前递交投标文件。

二、原 5 月 24 日本项目更正公告附件中：

四、提交投标文件截止时间、开标时间和地点

提交投标文件截止时间：2026-06-26 10:00:00（北京时间）

投标地点：上海政府采购网（www.zfcg.sh.gov.cn）

开标时间：2026-06-26 10:00:00

开标地点：上海政府采购网（www.zfcg.sh.gov.cn）

现更正为：

四、提交投标文件截止时间、开标时间和地点

提交投标文件截止时间：2026-07-13 10:00:00（北京时间）

投标地点：上海政府采购网（www.zfcg.sh.gov.cn）

开标时间：2026-07-13 10:00:00

开标地点：上海政府采购网（www.zfcg.sh.gov.cn）

三、原招标文件第 87 页 3.1.3 门诊病房终端中

14	床旁屏	安装于住院病区患者床旁，用于患者信息展示、呼叫对讲、信息查询、健康宣教等信息；
		屏幕尺寸≥13.3 寸触摸横屏；
		CPU 核数≥4 核；内存≥2GB；存储≥16G；
		系统：内置操作系统；
		支持 POE 供电或 12V DC 集中供电。
		网络接口：1000Mbps 以太网接口。
		蓝牙 5.0；支持 2.4G 和 5.8G 双频 WIFI；支持 NFC 识别医护人员工卡；
		内置麦克风，降噪防啸叫高清通话；内置喇叭；
		#为保障医院临床护理业务的高效开展，实现生命体征数据的自动化采集与精准关联，设备须内置 925MHz 超高频无线射频识别模块。该模块需支持在≥20cm 距离，以非接触式方式稳定识别床位标签，从而实现体温计、血压计、血氧仪、血糖仪等生命体征点测设备的数据自动采集与关联，确保数据源头准确，避免人工录入误差。

现更正为：

14	床旁屏	安装于住院病区患者床旁，用于患者信息展示、呼叫对讲、信息查询、健康宣教等信息；
		屏幕尺寸≥13.3 寸触摸横屏；
		CPU 核数≥4 核；内存≥2GB；存储≥16G；
		系统：内置操作系统；
		支持 POE 供电或 12V DC 集中供电。

		网络接口：1000Mbps 以太网接口。
		蓝牙 5.0；支持 2.4G 和 5.8G 双频 WIFI；支持 NFC 识别医护人员工卡；
		内置麦克风，降噪防啸叫高清通话；内置喇叭；

四、原招标文件第 97 页 3.1.5 网络设备中

14	内部业务网医疗区域无线接入点	本次无线接入点用于医疗机构复杂室内环境，为保障无线信号连续覆盖、无盲区、低时延、高稳定，满足医疗移动查房、移动护理、PACS 影像调阅、物联网设备并发接入等高可靠性要求，需对设备关键频段的天线增益性能提出最低限值要求。 #接入点频段及增益要求： 1、为保障医院生命体征监护、无线传声器及病床遥控等专用场景的稳定使用，频段增益要求：470MHz：≥2.5dBi、630MHz：≥3.0dBi、798MHz：≥6.5dBi 2、为保障医院 WIFI 2.4G 业务（如移动护理终端、PDA、查房平板）连接稳定、蓝牙设备（如蓝牙体温仪、血糖仪等）使用稳定，频段增益要求：1447MHz：≥5.5dBi、2400MHz：≥6.0dBi、2483MHz：≥5.5dBi 3、为保障医院 5G 信号（如远程会诊、大影像传输）使用稳定，频段增益要求：3300MHz：≥6.0dBi、3600MHz：≥5.5dBi 4、为保障医院 WIFI 5G 业务（如手术示教、医生移动工作站）连接稳定、高密连接（如门诊大厅、会议室、候诊区）使用稳定，频段增益要求：5850MHz：≥6.5dBi、6000MHz：≥6.0dBi；
		#为保障医院重症监护及生命体征监测等关键业务的数据传输稳定性，避免公共频段信号干扰，需具备生物医学遥测通信能力。频率需支持 608-630MHz 生物医学遥测专用频段；或采用其他抗干扰能力相当的专用无线通信技术（投标人需提供技术原理说明及抗干扰测试报告）。若采用 608-630MHz 频段，其发射功率、载频容限、占用带宽及杂散发射等指标须符合《工业和信息化部公告 2019 年第 52 号》中关于‘生物医学遥测设备’的技术要求。
		需与内部业务网无线控制器实现无缝兼容，支持被内部业务网无线控制器统一纳管，实现统一管理、配置下发、版本升级、射频管理等。
15	内部业务网无线接入中心	一体化无线接入中心设备，与无线接入点相连，无线网络和物联网可并发使用；
		CPU：主频≥1.5GHz，≥4 核；≥1G RAM/8G ROM；
		支持 IEEE802.11ax；支持 160MHz、80MHz 频宽模式；

		网络接口≥1 个 2.5G 网口；≥1 个自适应 100M/1000M 以太网，支持 POE+供电；
		≥8 个 400-7125MHz 射频输出口，支持外接子中心，≥8 个射频输出口同时具备对外直流供电能力；
		病房内 2.4GHz 及 5GHz 无线信号强度≥-75dBm，并满足同时实现单一病区内移动终端零漫游，零切换；
		支持通过射频口给无线接入点供电；
		支持 WPA2/WPA3 企业级认证，支持 MAC 认证：支持账号+密码+MAC+ESSID 绑定认证，限制终端使用指定账号+密码在限定 ESSID 下认证上网；
		支持通过管理平台监控设备运行状态，实现无线网、物联网统一监控；
		内置生物医学遥测模块，频率范围：至少满足 608-630MHz；
		支持物联网控制器平台协同处理定位数据，支持蓝牙+红外/低频定位数据通信；
		支持转发输液监控、冷链管理、环境监控系统数据功能；
		支持转发资产类定位、围术期定位、人员定位系统数据功能；
		需与内部业务网无线控制器实现无缝兼容，支持被内部业务网无线控制器统一纳管，实现统一管理、配置下发、版本升级、射频管理等。
16	住院区域无线接入点	本次无线接入点用于医疗机构复杂室内环境，为保障无线信号连续覆盖、无盲区、低时延、高稳定，满足医疗移动查房、移动护理、PACS 影像调阅、物联网设备并发接入等高可靠性要求，需对设备关键频段的天线增益性能提出最低限值要求。 接入点频段及增益要求： 1、为保障医院生命体征监护、无线传声器及病床遥控等专用场景的稳定使用，频段增益要求：470MHz：≥2.5dBi、630MHz：≥3.0dBi、798MHz：≥6.5dBi 2、为保障医院 WIFI 2.4G 业务（如移动护理终端、PDA、查房平板）连接稳定、蓝牙设备（如蓝牙体温仪、血糖仪等）使用稳定，频段增益要求：1447MHz：≥5.5dBi、2400MHz：≥6.0dBi、2483MHz：≥5.5dBi 3、为保障医院 5G 信号（如远程会诊、大影像传输）使用稳定，频段增益要求：3300MHz：≥6.0dBi、3600MHz：≥5.5dBi 4、为保障医院 WIFI 5G 业务（如手术示教、医生移动工作站）连接稳定、高密连接使用稳定，频段增益要求：5850MHz：≥6.5dBi、6000MHz：≥6.0dBi；

		具备蓝牙定位功能；
		为保障医院重症监护及生命体征监测等关键业务的数据传输稳定性，避免公共频段信号干扰，需具备生物医学遥测通信能力。频率需支持 608-630MHz 生物医学遥测专用频段；或采用其他抗干扰能力相当的专用无线通信技术（投标人需提供技术原理说明及抗干扰测试报告）。若采用 608-630MHz 频段，其发射功率、载频容限、占用带宽及杂散发射等指标须符合《工业和信息化部公告 2019 年第 52 号》中关于‘生物医学遥测设备’的技术要求。
		具备定位数据通信功能，支持定位数据上报与与定位指令下发，通信速率≥200Kbps；
		需与内部业务网无线控制器实现无缝兼容，支持被内部业务网无线控制器统一纳管，实现统一管理、配置下发、版本升级、射频管理等。

现更正为

14	内部业务网医疗区域无线接入点	需与内部业务网无线控制器实现无缝兼容，支持被内部业务网无线控制器统一纳管，实现统一管理、配置下发、版本升级、射频管理等。
		支持 IEEE 802.11be 标准，兼容 IEEE 802.11a/b/g/n/ac/ax 标准
		速率≥3Gbps
		支持 802.1x 认证、MAC 地址认证、Portal 认证等
		可扩展多种标准的物联协议，包括 RFID，ZigBee 等物联网协议。
15	内部业务网无线接入中心	一体化无线接入中心设备，与无线接入点相连，无线网络和物联网可并发使用；
		支持 IEEE802.11ax；支持 160MHz、80MHz 频宽模式；
		网络接口≥1 个 2.5G 网口；≥1 个自适应 100M/1000M 以太网，支持 POE+供电；
		病房内 2.4GHz 及 5GHz 无线信号强度≥-75dBm，并满足同时实现单一病区内移动终端零漫游，零切换；
		支持通过管理平台监控设备运行状态，实现无线网、物联网统一监控；
		支持物联网控制器平台协同处理定位数据；
		可扩展多种标准的物联协议，包括 RFID，ZigBee 等物联网协议。
		需与内部业务网无线控制器实现无缝兼容，支持被内部业务网无线控制器统一纳管，实现统一管理、配置下发、版本升级、射频管理等。
16	住院区域	具备蓝牙定位功能；

	无线接入点	具备定位数据通信功能，支持定位数据上报与与定位指令下发，通信速率≥200Kbps；
		支持 IEEE 802.11be 标准，兼容 IEEE 802.11a/b/g/n/ac/ax 标准
		速率≥3Gbps
		支持 802.1x 认证、MAC 地址认证、Portal 认证等
		需与内部业务网无线控制器实现无缝兼容，支持被内部业务网无线控制器统一纳管，实现统一管理、配置下发、版本升级、射频管理等。

五、原招标文件第 272 页 3.4.2 商用密码

序号	名称	技术参数
1	密码服务管理平台	★提供由国家密码管理局颁发的商用密码产品认证证书
		提供统一的身份认证、签名验签、数据加解密等密码服务；
		提供统一密码服务接口，对密码服务及设备进行统一监控、运维及配置管理，提供密钥全生命周期管理；
		支持实时监控密码设备，监控信息包括内存、硬盘、CPU、设备状态、资源状态、服务状态等；
		支持国密 SM2、SM3、SM4 算法；
		支持 PDF 格式文档的数字签名与验签功能；
		支持主流签名服务器接口，提供包括签名、验签、加密、解密、HMAC、数字信封等在内的通用密码运算能力，可对接不同厂商的签名服务器或密码设备；
		支持签名、验签、加密、解密、HMAC、数字信封等功能的纯软件方式实现，满足无硬件依赖场景下的密码运算需求；

		支持 XML 数字签名，包括封内签名、封外签名、分离签名等多种形态的签名与验签；
		提供安全便捷高效的加解密服务，降低应用系统对接复杂度，支持底层加密运算在后台密码设备（如密码机、密码卡）中完成；
		支持通过统一门户进行密钥全生命周期管理，并支持基于权限、角色的用户分级安全管理；
		支持通用类型密钥的生成，密钥种类包括：国际 RSA 算法、国密 SM2 算法等非对称密钥，国际 AES 算法、国密 SM4 算法等对称密钥；
		支持密钥库管理功能，具备密钥分发与密钥同步能力；
		提供多业务管理后台（Portal），具备统一的安全授权管理、统一业务配置、统一告警监控能力；
		支持多种业务接入模式，包括透传模式、服务代理模式等；其中透传模式下业务系统零改造即可接入，其他模式下平台应提供业务监控、态势感知等可视化展示能力；
		平台自身须满足以下等保密评三级安全要求：敏感数据加密存储、关键数据传输通道加密、支持数字证书双因素登录、支持白名单和 TOKEN 等授权访问机制、确保日志记录的完整性保护、具备对关键数据和应用程序的完整性校验能力、提供安全接入机制；
		产品兼容国产服务器环境。
4	数据库加密与访问控制系统	★提供由国家密码管理局颁发的商用密码产品认证证书
		机架式设备：冗余电源；内存≥16G；接口≥6 个千兆电口，4 个千兆光口；≥1T 硬盘；支持双机热备或集群部署；
		最大密钥存储容量不少于 100,000，最大在线加解密吞吐量不少于 400Mbps；

		无需修改业务系统代码，实现数据库数据的存储机密性和完整性保护，实现透明加密，支持 SM2、SM3、SM4 等商用密码算法；
		支持多种加密模式，支持业务在线加密，不需要业务停机；
		支持基于身份的密文访问控制，身份要素至少包括 IP 地址、主机名、操作系统账户、数据库账户等，根据用户权限进行数据库返回结果控制，只有拥有合法权限的数据库用户才可看到明文，无合法权限的用户返回经过加密的数据或禁止访问；
		支持旁路模式部署，兼容主流国产以及非国产数据库；
		支持对称密钥和非对称密钥的全生命周期管理，包括密钥生成、启用、禁用、备份、恢复、归档、还原、删除等操作；支持以密钥分量模式导入/导出根密钥，支持以密码信封模式导入/导出对称密钥；
		支持设置密钥计划删除周期，并对系统内近几天内即将被删除的密钥进行告警提示；
		支持对称密钥及非对称密钥两种加解密方式对结构化数据与非结构化数据进行加解密操作；
		支持数据库中明文数据与密文数据的识别与区分展示；
		支持业务代码无侵入的透明 HMAC 完整性校验功能，支持手动校验与定时校验两种模式，用于检测数据是否被篡改；
		支持基于角色的访问控制，实现系统管理员、安全管理员、审计管理员等角色的权限分离与划分；
		支持基于属性的访问控制，具备应用密钥操作权限管理、应用 IP 白名单管理以及资源访问控制能力；
		支持基于硬件特征的白名单授权机制，可对 CPU 序列号、内存序列号等硬件信息进行绑定授权；

		支持系统数据的备份与恢复，支持系统的跨版本升级与恢复，支持全量升级及补丁包升级。
5	移动身份认证网关	★提供由国家密码管理局颁发的商用密码产品认证证书
		机架式设备：冗余电源；内存≥16G；接口≥4 个千兆网口；支持双机热备或集群部署；
		认证事务处理能力≥6000TPS；国密吞吐量≥200Mbps；最大并发连接数≥8000；每秒新建连接数≥2800；
		为用户提供安全接入通道;为业务系统提供基于国密数字证书的身份认证、SSL 隧道加密等功能；
		支持设置预警状态监控，管理员可以设置 CPU、磁盘、内存、网络流量预警、业务日志、在线连接数、在线用户监控的预警状态信息功能；
		支持对接主流 CA 机构签发移动证书；
		为业务系统提供统一的服务接口，实现认证能力的标准化对接；
		移动数字证书支持 SM2、SM3、SM4 等密码算法；
		支持国产密码算法（SM2、SM3、SM4）及国际密码算法进行安全传输；
		支持与各类移动业务系统无缝对接，认证方式包括动态口令、数字证书、二维码等多种方式；
		提供完整的 PC 端安全开发套件，便于用户进行业务定制开发；开放协同签名、扫码签章、二维码扫描、动态口令、签名验签、证书下载及证书生命周期管理等接口供客户集成调用；
		PC 登录认证支持生成二维码扫码登录认证、推送登录认证、获取 PC 登录密码、忘记 PC 密码等；
		通信支持国际算法与国密算法的单向及双向 SSL/TLS 通道建立，不依

		赖外部 SSL 设备独立实现。

更正为：

序号	名称	技术参数
1	密码服务管理平台	★提供由国家密码管理局颁发的商用密码产品认证证书
		提供统一的身份认证、签名验签、数据加解密等密码服务；
		提供统一密码服务接口，对密码服务及设备进行统一监控、运维及配置管理，提供密钥全生命周期管理；
		支持实时监控密码设备，监控信息包括内存、硬盘、CPU、设备状态、资源状态、服务状态等；
		支持国密 SM2、SM3、SM4 算法；
		支持 PDF 格式文档的数字签名与验签功能；
		支持主流签名服务器接口，提供包括签名、验签、加密、解密、HMAC、数字信封等在内的通用密码运算能力，可对接不同厂商的签名服务器或密码设备；
		支持签名、验签、加密、解密、HMAC、数字信封等功能的纯软件方式实现，满足无硬件依赖场景下的密码运算需求；
		提供安全便捷高效的加解密服务，降低应用系统对接复杂度，支持底层加密运算在后台密码设备（如密码机、密码卡）中完成；
		支持通过统一门户进行密钥全生命周期管理，并支持基于权限、角色的用户分级安全管理；
		支持通用类型密钥的生成，密钥种类包括：国际 RSA 算法、国密 SM2 算法等非对称密钥，国际 AES 算法、国密 SM4 算法等对称密钥；
		提供多业务管理后台（Portal），具备统一的安全授权管理、统一业务配置、统一告警监控能力；

		支持多种业务接入模式，包括透传模式、服务代理模式等；其中透传模式下业务系统零改造即可接入，其他模式下平台应提供业务监控、态势感知等可视化展示能力；
		产品兼容国产服务器环境。
		#支持 XML 数字签名，包括封内签名、封外签名、分离签名等多种形态的签名与验签； 支持密钥库管理功能，具备密钥分发与密钥同步能力； 平台自身须满足以下等保密评三级安全要求：敏感数据加密存储、关键数据传输通道加密、支持数字证书双因素登录、支持白名单和 TOKEN 等授权访问机制、确保日志记录的完整性保护、具备对关键数据和应用程序的完整性校验能力、提供安全接入机制； （提供的证明材料需包含以上全部参数，未提供或提供不全视为不响应）
4	数据库加密与访问控制系统	★提供由国家密码管理局颁发的商用密码产品认证证书
		机架式设备：冗余电源；内存≥16G；接口≥6 个千兆电口，4 个千兆光口；≥1T 硬盘；支持双机热备或集群部署；
		最大密钥存储容量不少于 100,000，最大在线加解密吞吐量不少于 400Mbps；
		支持多种加密模式，支持业务在线加密，不需要业务停机；
		支持基于身份的密文访问控制，身份要素至少包括 IP 地址、主机名、操作系统账户、数据库账户等，根据用户权限进行数据库返回结果控制，只有拥有合法权限的数据库用户才可看到明文，无合法权限的用户返回经过加密的数据或禁止访问；
		支持旁路模式部署，兼容主流国产以及非国产数据库；
		支持设置密钥计划删除周期，并对系统内近几天内即将被删除的密钥

		进行告警提示；
		支持对称密钥及非对称密钥两种加解密方式对结构化数据与非结构化数据进行加解密操作；
		支持数据库中明文数据与密文数据的识别与区分展示；
		支持业务代码无侵入的透明 HMAC 完整性校验功能，支持手动校验与定时校验两种模式，用于检测数据是否被篡改；
		支持基于角色的访问控制，实现系统管理员、安全管理员、审计管理员等角色的权限分离与划分；
		支持基于属性的访问控制，具备应用密钥操作权限管理、应用 IP 白名单管理以及资源访问控制能力；
		支持系统数据的备份与恢复，支持系统的跨版本升级与恢复，支持全量升级及补丁包升级。
		#无需修改业务系统代码，实现数据库数据的存储机密性和完整性保护，实现透明加密，支持 SM2、SM3、SM4 等商用密码算法； 支持基于硬件特征的白名单授权机制，可对 CPU 序列号、内存序列号等硬件信息进行绑定授权； 支持对称密钥和非对称密钥的全生命周期管理，包括密钥生成、启用、禁用、备份、恢复、归档、还原、删除等操作；支持以密钥分量模式导入/导出根密钥，支持以密码信封模式导入/导出对称密钥； （提供的证明材料需包含以上全部参数，未提供或提供不全视为不响应）
5	移动身份认证网关	★提供由国家密码管理局颁发的商用密码产品认证证书
		机架式设备；冗余电源；内存≥16G；接口≥4 个千兆网口；支持双机热备或集群部署；
		认证事务处理能力≥6000TPS；国密吞吐量≥200Mbps；最大并发连接

		数≥8000；每秒新建连接数≥2800；
		为用户提供安全接入通道;为业务系统提供基于国密数字证书的身份认证、SSL 隧道加密等功能；
		支持设置预警状态监控，管理员可以设置 CPU、磁盘、内存、网络流量预警、业务日志、在线连接数、在线用户监控的预警状态信息功能；
		支持对接主流 CA 机构签发移动证书；
		为业务系统提供统一的服务接口，实现认证能力的标准化对接；
		移动数字证书支持 SM2、SM3、SM4 等密码算法；
		支持国产密码算法（SM2、SM3、SM4）及国际密码算法进行安全传输；
		通信支持国际算法与国密算法的单向及双向 SSL/TLS 通道建立，不依赖外部 SSL 设备独立实现。
		#支持与各类移动业务系统无缝对接，认证方式包括动态口令、数字证书、二维码等多种方式； 提供完整的 PC 端安全开发套件，便于用户进行业务定制开发；开放协同签名、扫码签章、二维码扫描、动态口令、签名验签、证书下载及证书生命周期管理等接口供客户集成调用； PC 登录认证支持生成二维码扫码登录认证、推送登录认证、获取 PC 登录密码、忘记 PC 密码等； （提供的证明材料需包含以上全部参数，未提供或提供不全视为不响应）

六、原招标文件第 290 页 6.#项要求汇总表

序号	板块	系统名称	技术要求	证明材料

1	#项	内网核心交换机	机架式设备，实配主控引擎≥2、电源≥4个（支持N+N冗余），业务插槽数量≥8，配置40G以上堆叠线缆； 框式核心交换机：交换容量≥1600Tbps，包转发率≥440000Mpps； 实配端口≥96个万兆光口，≥48个千兆电口，≥4个40GE光口，支持40G/100G端口扩展，40G多模QSFP+光模块≥2个； IPv4转发信息库路由容量不低于200万条；支持基于IPv6的段路由尽力而为转发模式；支持链路聚合技术，可实现跨设备的链路带宽叠加与冗余备份（如M-LAG、堆叠链路聚合等方案均可）。（提供的证明材料需包含以上全部参数，未提供或提供不全视为不响应）	提供所投产品官网产品页面截图（含链接）或产品说明书扫描件或原厂盖章的参数证明
2	#项	内部业务网医疗区域无线接入点	接入点频段及增益要求：1、为保障医院生命体征监护、无线传声器及病床遥控等专用场景的稳定使用，频段增益要求如下：470MHz：≥2.5dBi、630MHz：≥3.0dBi、798MHz：≥6.5dBi； 2、为保障医院WIFI 2.4G业务（如移动护理终端、PDA、查房平板）连接稳定、蓝牙设备（如蓝牙体温仪、血糖仪等）使用稳定，频段增益要求如下：1447MHz：≥5.5dBi、2400MHz：≥6.0dBi、2483MHz：≥5.5dBi； 3、为保障医院5G信号（如远程会诊、大影像传输）使用稳定，频段增益要求如下：3300MHz：≥6.0dBi、3600MHz：≥5.5dBi； 4、为保障医院WIFI 5G业务（如手术示教、医生移动工作站）连接稳定、高密连接（如门诊大厅、会议室、候诊区）使用稳定，频段增益要求如下：5850MHz：≥6.5dBi、6000MHz：≥6.0dBi；（提供的证明材料需包含以上全部参数，未提供或提供不全视为不响应）	提供国家认可的检测机构出具的检测报告

3			为保障医院重症监护及生命体征监测等关键业务的数据传输稳定性，避免公共频段信号干扰，所投产品需具备生物医学遥测通信能力。 频率要求：支持 608-630MHz 生物医学遥测专用频段；或采用其他抗干扰能力相当的专用无线通信技术（投标人需提供技术原理说明及抗干扰测试报告）。若采用 608-630MHz 频段，其发射功率、载频容限、占用带宽及杂散发射等指标须符合《工业和信息化部公告 2019 年第 52 号》中关于‘生物医学遥测设备’的技术要求。	提供国家认可的检测机构出具的检测报告
4	#项	超融合软件系统	数据本地化：考虑到医院业务系统高并发、低时延、连续运行需求，底层存储应支持数据本地化读写优化策略，可优先将虚拟机业务数据写入当前节点本地存储，虚拟机迁移后其数据可自动渐进式迁移至当前物理节点，实现数据就近存储与访问，确保最短 I/O 路径、降低访问延迟并减少集群网络流量。	提供国家认可的检测机构出具的检测报告。
5			高可靠性要求：为保障医院关键业务持续可用，平台应支持虚拟机高可用机制，节点故障触发切换时，可自定义虚拟机业务恢复优先级，并按照设定优先级顺序执行恢复操作，优先保障核心业务系统快速恢复。	提供国家认可的检测机构出具的检测报告。
6	#项	床旁屏	为保障医院临床护理业务的高效开展，实现生命体征数据的自动化采集与精准关联，设备须内置 925MHz 超高频无线射频识别模块。该模块需支持在≥20cm 距离，以非接触式方式稳定识别床位标签，从而实现体温计、血压计、血氧仪、血糖仪等生命体征点测设备的数据自动采集与关联，确保数据源头准确，避免人工录入误差。	提供国家认可的检测机构出具的检测报告。
7	#项	核心防火墙	为保障医院核心业务的网络访问质量，实现基于业务类型的精细化流量调度，须支持基于统一资源定位符（URL）的策略路由功能。设备应能识别应用层域名信息，并根据预设策略将访问特定业务网站（如医保）的流量强制牵引至	提供国家认可的检测机构出具的检测报告

			专用链路或最优出口，确保关键业务传输的低延迟与高稳定性。	
8	#项	内网潜伏威胁探针	鉴于医院 HIS 系统、门户网站及对外服务平台承载着大量敏感患者数据且面临复杂的互联网攻击风险，为防止黑客利用 Web 漏洞植入后门程序导致数据泄露或业务系统被非法控制，设备需具备针对加密隐蔽通道的检测能力。设备应具备智能威胁检测机制，能够识别 Webshell（网页后门）的通信行为。针对黑客利用加密工具进行隐蔽通信的场景，设备需具备有效的识别与发现能力，防止传统特征库无法检测的加密流量攻击。	提供国家认可的检测机构出具的检测报告
9	#项	安全隔离与信息交换系统	为保障医院核心业务网（如 HIS、EMR）与外部网络（如互联网、医保网）进行数据交换时的安全性，防止恶意文件利用伪装手段穿透边界，系统须能检测并拦截后缀名与文件实际内容不符的伪造文件，防止恶意代码植入。支持对传输文件进行内容合规性检查，能够检测文件中是否包含异常的二进制执行代码、恶意脚本或非法嵌入对象。当发现文件内容与标称类型不符或包含潜在威胁代码时，系统应能自动阻断传输。	提供国家认可的检测机构出具的检测报告
10	#项	堡垒机	为防范非法利用遗留账号窃取或篡改患者诊疗数据、医保信息等敏感信息，系统应支持对闲置账号、未清理账号、未纳管账号等异常账号进行自动稽核与风险识别，并支持导出异常账号稽核报告，便于管理员全面掌握账号安全状态并开展定期清理与权限整改工作；	提供国家认可的检测机构出具的检测报告
11	#项	日志审计系统	医院核心业务系统日均产生海量日志数据，为提升医院安全运营效率，降低告警噪音干扰，产品须支持关联分析结果的告警重定义功能，能够对关联规则触发的告警事件关键字段进行灵活修订，如告警级别和告警类型；	提供国家认可的检测机构出具的检测报告
12	#项	入侵防御系统	为保障医院网络稳定运行，保护医院 CPU 资源，降低业务中断风险及不合理电费消耗，需具备对挖矿木马进行重点	提供国家认可的检测机构出

			专项防护的能力，支持挖矿行为的实时检测与主动防护，并生成挖矿行为日志，日志可通过源地址、目的地地址和信誉等级进行查询，展示挖矿日志的威胁类型、挖矿值及协议等；	具的检测报告
13	#项	中心机房UPS	考虑到医院手术室、ICU、重症监护室、影像科（CT/MRI）、检验科等关键业务区域对供电连续性与电能质量具有极高要求——谐波污染可能干扰精密医疗设备正常运行，功率因数过低会增加线路损耗及引发供电系统过热风险，逆变效率低下将显著增加长期运营电费成本，输出波形失真则可能导致设备误动作或损坏，UPS 产品需满足： 整流器输入性能：应符合 YD/T 2165-2010《通信用模块化不间断电源》标准要求。 输入谐波电流总含量：在 25%～100%负载率下，要求不大于 3%。 输入功率因数：在 25%～100%负载率下，要求不低于 0.99。 市电模式下在线逆变系统效率： 100%负载下，系统效率 ＞ 96%； 50%负载下，系统效率 ＞ 96.5%； 25%负载下，系统效率 ＞ 95.5%。 输出波形质量：输出波形为连续正弦波。在带 100%不均衡负载时，波形失真度要求：线性负载 ≤ 1.5%，非线性负载 ≤ 2.0%。 （提供的证明材料需包含以上全部参数，未提供或提供不全视为不响应）	提供国家认可的检测机构出具的检测报告
14	#项	模块化机房行间精密空调	考虑到医院核心信息机房承载着 HIS、EMR、LIS、PACS 等关键业务系统的服务器、存储及网络设备，这些设备 7×24 小时不间断运行，对机房环境温湿度及散热能力具有极高要求——能效比过低会导致长期运营电费显著增加，不符合绿色医院建设要求；风量不足则无法有效带走设备密	提供国家认可的检测机构出具的检测报告

			集区域的热量，可能引发设备过热、宕机甚至损坏，直接影响临床诊疗业务的连续性和患者安全——因此对产品提出以下强制性技术指标要求：整机能效比：≥ 4.0；风量：≥ 8500m³/h（立方米/小时）。	
15	#项	中心机房节能要求	医院的核心医疗业务需7×24小时不间断运行，且白天门诊高峰与夜间低负载时段并存，为降低数据中心长期电费支出、提升节能水平，要求模块化机房在25%、50%、75%、100%四种负载率下的全年平均能源使用效率测试结果均＜1.3。	提供国家认可的检测机构出具的检测报告

更正为：

序号	板块	系统名称	技术要求	证明材料
1	#项	内网核心交换机	机架式设备，实配主控引擎≥2、电源≥4个（支持N+N冗余），业务插槽数量≥8，配置40G以上堆叠线缆； 框式核心交换机：交换容量≥1600Tbps，包转发率≥440000Mpps； 实配端口≥96个万兆光口，≥48个千兆电口，≥4个40GE光口，支持40G/100G端口扩展，40G多模QSFP+光模块≥2个； IPv4转发信息库路由容量不低于200万条；支持基于IPv6的段路由尽力而为转发模式；支持链路聚合技术，可实现跨设备的链路带宽叠加与冗余备份（如M-LAG、堆叠链路聚合等方案均可）。（提供的证明材料需包含以上全部参数，未提供或提供不全视为不响应）	提供所投产品官网产品页面截图（含链接）或产品说明书扫描件或原厂盖章的参数证明
2	#项	超融合软件系统	数据本地化：考虑到医院业务系统高并发、低时延、连续运行需求，底层存储应支持数据本地化读写优化策略，可优先将虚拟机业务数据写入当前节点本地存储，虚拟机迁移后其数据可自动渐进式迁移至当前物理节点，实现数据就近存储与访问，确保最短I/O路径、降低访问延迟并减少集群网络流量。	提供国家认可的检测机构出具的检测报告。

3			高可靠性要求：为保障医院关键业务持续可用，平台应支持虚拟机高可用机制，节点故障触发切换时，可自定义虚拟机业务恢复优先级，并按照设定优先级顺序执行恢复操作，优先保障核心业务系统快速恢复。	提供国家认可的检测机构出具的检测报告。
4	#项	核心防火墙	为保障医院核心业务的网络访问质量，实现基于业务类型的精细化流量调度，须支持基于统一资源定位符（URL）的策略路由功能。设备应能识别应用层域名信息，并根据预设策略将访问特定业务网站（如医保）的流量强制牵引至专用链路或最优出口，确保关键业务传输的低延迟与高稳定性。	提供国家认可的检测机构出具的检测报告
5	#项	内网潜伏威胁探针	鉴于医院 HIS 系统、门户网站及对外服务平台承载着大量敏感患者数据且面临复杂的互联网攻击风险，为防止黑客利用 Web 漏洞植入后门程序导致数据泄露或业务系统被非法控制，设备需具备针对加密隐蔽通道的检测能力。设备应具备智能威胁检测机制，能够识别 Webshell（网页后门）的通信行为。针对黑客利用加密工具进行隐蔽通信的场景，设备需具备有效的识别与发现能力，防止传统特征库无法检测的加密流量攻击。	提供国家认可的检测机构出具的检测报告
6	#项	安全隔离与信息交换系统	为保障医院核心业务网（如 HIS、EMR）与外部网络（如互联网、医保网）进行数据交换时的安全性，防止恶意文件利用伪装手段穿透边界，系统须能检测并拦截后缀名与文件实际内容不符的伪造文件，防止恶意代码植入。支持对传输文件进行内容合规性检查，能够检测文件中是否包含异常的二进制执行代码、恶意脚本或非法嵌入对象。当发现文件内容与标称类型不符或包含潜在威胁代码时，系统应能自动阻断传输。	提供国家认可的检测机构出具的检测报告
7	#项	堡垒机	为防范非法利用遗留账号窃取或篡改患者诊疗数据、医保信息等敏感信息，系统应支持对闲置账号、未清理账号、未纳管账号等异常账号进行自动稽核与风险识别，并支持	提供国家认可的检测机构出具的检测报告

			导出异常账号稽核报告，便于管理员全面掌握账号安全状态并开展定期清理与权限整改工作；	
8	#项	日志审计系统	医院核心业务系统日均产生海量日志数据，为提升医院安全运营效率，降低告警噪音干扰，产品须支持关联分析结果的告警重定义功能，能够对关联规则触发的告警事件关键字段进行灵活修订，如告警级别和告警类型；	提供国家认可的检测机构出具的检测报告
9	#项	入侵防御系统	为保障医院网络稳定运行，保护医院 CPU 资源，降低业务中断风险及不合理电费消耗，需具备对挖矿木马进行重点专项防护的能力，支持挖矿行为的实时检测与主动防护，并生成挖矿行为日志，日志可通过源地址、目的地地址和信誉等级进行查询，展示挖矿日志的威胁类型、挖矿值及协议等；	提供国家认可的检测机构出具的检测报告
10	#项	中心机房UPS	考虑到医院手术室、ICU、重症监护室、影像科（CT/MRI）、检验科等关键业务区域对供电连续性与电能质量具有极高要求——谐波污染可能干扰精密医疗设备正常运行，功率因数过低会增加线路损耗及引发供电系统过热风险，逆变效率低下将显著增加长期运营电费成本，输出波形失真则可能导致设备误动作或损坏，UPS 产品需满足： 整流器输入性能：应符合 YD/T 2165-2010《通信用模块化不间断电源》标准要求。 输入谐波电流总含量：在 25%～100%负载率下，要求不大于 3%。 输入功率因数：在 25%～100%负载率下，要求不低于 0.99。 市电模式下在线逆变系统效率： 100%负载下，系统效率 > 96%； 50%负载下，系统效率 > 96.5%； 25%负载下，系统效率 > 95.5%。 输出波形质量：输出波形为连续正弦波。在带 100%不均衡负载时，波形失真度要求：线性负载 ≤ 1.5%，非线性负	提供国家认可的检测机构出具的检测报告

			载 ≤ 2.0%。 （提供的证明材料需包含以上全部参数，未提供或提供不全视为不响应）	
11	#项	模块化机房行间精密空调	考虑到医院核心信息机房承载着 HIS、EMR、LIS、PACS 等关键业务系统的服务器、存储及网络设备，这些设备 7×24 小时不间断运行，对机房环境温湿度及散热能力具有极高要求——能效比过低会导致长期运营电费显著增加，不符合绿色医院建设要求；风量不足则无法有效带走设备密集区域的热量，可能引发设备过热、宕机甚至损坏，直接影响临床诊疗业务的连续性和患者安全——因此对产品提出以下强制性技术指标要求：整机能效比：≥ 4.0；风量：≥ 8500m³/h（立方米/小时）。	提供国家认可的检测机构出具的检测报告
12	#项	中心机房节能要求	医院的核心医疗业务需 7×24 小时不间断运行，且白天门诊高峰与夜间低负载时段并存，为降低数据中心长期电费支出、提升节能水平，要求模块化机房在 25%、50%、75%、100%四种负载率下的全年平均能源使用效率测试结果均＜1.3。	提供国家认可的检测机构出具的检测报告
13	#项	密码服务管理平台	支持 XML 数字签名，包括封内签名、封外签名、分离签名等多种形态的签名与验签； 支持密钥库管理功能，具备密钥分发与密钥同步能力； 平台自身须满足以下等保密评三级安全要求：敏感数据加密存储、关键数据传输通道加密、支持数字证书双因素登录、支持白名单和 TOKEN 等授权访问机制、确保日志记录的完整性保护、具备对关键数据和应用程序的完整性校验能力、提供安全接入机制； （提供的证明材料需包含以上全部参数，未提供或提供不全视为不响应）	提供国家认可的检测机构出具的检测报告
14	#项	数据库加密与访问	#无需修改业务系统代码，实现数据库数据的存储机密性和完整性保护，实现透明加密，支持 SM2、SM3、SM4 等商	提供国家认可的检测机构出

		控制系统	用密码算法； 支持基于硬件特征的白名单授权机制，可对 CPU 序列号、内存序列号等硬件信息进行绑定授权； 支持对称密钥和非对称密钥的全生命周期管理，包括密钥生成、启用、禁用、备份、恢复、归档、还原、删除等操作；支持以密钥分量模式导入/导出根密钥，支持以密码信封模式导入/导出对称密钥； （提供的证明材料需包含以上全部参数，未提供或提供不全视为不响应）	具的检测报告
15	#项	移动身份认证网关	支持与各类移动业务系统无缝对接，认证方式包括动态口令、数字证书、二维码等多种方式； 提供完整的 PC 端安全开发套件，便于用户进行业务定制开发；开放协同签名、扫码签章、二维码扫描、动态口令、签名验签、证书下载及证书生命周期管理等接口供客户集成调用； PC 登录认证支持生成二维码扫码登录认证、推送登录认证、获取 PC 登录密码、忘记 PC 密码等； （提供的证明材料需包含以上全部参数，未提供或提供不全视为不响应）	提供国家认可的检测机构出具的检测报告

七：原招标文件第 284 页 4. 项目实施要求中

4.5 现场保障要求

数据迁移、系统割接、上线试运行期间，投标人须安排足额专业技术人员现场全程保障，确保过程顺利、不影响医院正常业务，并需提前做好大面积业务中断以及大面积断网应急预案。现场保障人员须具备对应岗位资质，名单及资质证明须提前提交招标人审核确认。

现更正为：

4.5 现场保障要求

数据迁移、系统割接、上线试运行期间，投标人须安排足额专业技术人员现场全程保障，确保过程顺利、不影响医院正常业务，并需提前做好大面积业务中断以及大面积断网应急预案。现场保障人员须具备对应岗位资质，名单及资质证明须提前提交招标人审核确认。

4.6 双方的权利义务

一、甲方权利与义务

1. 项目中标后，甲方积极协调原系统服务商配合本项目的数据迁移、接口对接相关工作。包括且不限于合规公开的数据库结构、数据字典、接口规范等项目必要的资料。

2. 免费提供施工场地、电力、网络及机房作业通行权限。

3. 为驻场人员提供临时办公场所，协助办理出入、准入手续。

4. 安排专职对接人，协调院内各科室配合测试、培训及验收。

5. 甲方对项目进度、施工质量、数据及资料使用进行全程监管。

二、乙方权利与义务

1. 所有技术资料、业务数据仅可用于本项目实施及质保服务。

2. 严格恪守保密规定，不得外泄、转借或挪作其他用途。

3. 项目竣工验收后，及时返还全部资料并彻底删除留存文件。

4. 乙方依托自身技术能力，完成全量数据迁移与系统联调对接。

5. 现场工作人员须严格遵守医院各项管理、安防及保密制度。

6. 若因乙方原因造成数据泄露、系统故障，由乙方承担全部责任。

7. 项目通过最终验收后，乙方须无条件向甲方完整交付本项目开发的全部软件源代码、编译脚本、开发配置文件等全套源码资产，确保交付源代码完整、真实、有效、可编译、可正常运行，无遗漏、无加密、无后门、无知识产权权属纠纷，全部源代码著作权及使用权归甲方所有，甲方享有永久、免费、完整的使用、修改、升级、二次开发及部署权限。

上海市松江区方塔中医医院

2026 年 6 月 22 日

上海市松江区政府采购中心

2026 年 6 月 22 日