|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **名称** | **参数** | **数量** |
| 1 | 远程会诊系统 | 下级医院医生无法针对患者病情下明确诊断，需要上级专家协助时，发起远程会诊预约申请，同时上传当前患者相关的病历资料，远程会诊人员审核后根据病情轻重程度安排远程会诊时间，远程会诊通过音视频在线互动的方式实现。 1.远程会诊支持离线会诊和在线交互会诊两种会诊模式。 2.支持会诊申请，申请的内容包括会诊的模式和方式、会诊时间、会诊专家、会诊费用（可根据会诊费用选择会诊规模、专家级别）、会诊病情描述和会诊原因等信息的录入； 3.支持会诊审核，在线会诊专家或者科室医务人员接收到会诊的申请信息时，查看并完善会诊资料（与所申请会诊医生共同完成），通过查看患者的病情程度确定会诊时间，如果病情比较紧急，则需要尽早安排会诊人员； 4.可实现多方参会专家在会诊过程中能同步查阅包括患者检查信息、医嘱信息、病例信息、治疗信息等数据，支撑多学科会诊的开展。 5.具备会诊协同文件共享体系，支持将患者临床诊疗信息、检查报告、图像共享给上级主管医生协同诊断，文件仅限于平台内点对点进行传输，不会被非授权人员获取，确保患者隐私数据安全性。 6.支持会诊管理，会诊管理中基层医生可以查看已经申请的会诊列表，会诊专家则可以看到同意或未同意的会诊申请单，进入申请单详情可以看到患者的基本信息和上传的病历资料； 7.会诊场景功能：支持进入会诊之后查看到申请会诊时的内容，包括患者基本信息、手动录入的病情资料、上传的附件、以及上传的检查检验等数据；同时支持打开第三方的电子病历浏览页面；支持打开音视频进行互动，在音视频界面中支持桌面共享、增加视频源、截图等功能，同时后台可以自动录像；会诊讨论后支持专家端编写会诊报告，申请端支持打开转诊页面进行转诊申请； 8.查看健康档案：通过接口将患者过往历史完成的健康档案信息包括：基本信息、历史检查检验信息、影像资料、病历记录、过敏史等内容； 9.支持多种会诊类型，包括临床会诊、影像会诊、病理会诊等。 10.所投产品内嵌影像前置统一网关系统，具备申请会诊患者历史检查记录进行影像归档、影像提取及应用信息管理的配置、提取及查询服务 11.影像会诊：影像会诊可与医疗集团内医院PACS系统集成，调阅患者信息及检查图像，检查图像通过DICOM方式获取，可调阅医院电子病历，进行综合诊断，包含了对影像的强大处理功能，需支持以下应用： 支持备注,定标,测量； 支持图像描述备注信息； 支持图像对比度快速调节、并可根据检查部位预设窗宽窗位值，自动调阅； 图像后处理功能包括：移动、缩放、放大镜、反片、顺、逆时针旋转、上下左右镜像、伪彩等； 标注功能包括：圆形、测量笔、箭头、文字、直线、长方形、多边形、角度等类型，各标注可以显示测量值，也可以隐藏测量值； 图像窗口布局：单幅、1X2幅、2X2幅、2X3幅、3X4幅、4X6幅、6X8幅和自定义显示等等； 支持可对请求端的图像会诊窗口同步显示。 具备标准化数据共享能力，在系统架构、数据中心、网络架构等基础条件允许情况下，可实现对影像数据、图像的跨机构存储与共享能力。 12.临床会诊：临床在线会诊提供给临床医生进行在线综合病历会诊，医生在会诊时调阅该病人的电子病历以做会诊依据，可查看电子病历，需支持以下应用： 能流畅、清晰的显示对方病历系统信息； 支持屏幕同步模式，同时可自行切换显示模式，包括自适应、原始比例以及全屏模式； 支持窗口同步模式； 对方可以同步准确的看到控制方在对图像做的任何操作； 方便查看对方编写报告和调阅电子病历等流程操作。 13.报告编写：会诊专家根据前面会诊之后，就可以得出会诊诊断结果。专家在这个会诊报告软件中编写并提交会诊报告，以便会诊的请求端查看会诊报告。需支持以下应用： 会诊方编写报告并归档； 可以自定义报告的模板； 可以自定义诊库的数据； 可以上传报告到服务器； 可以下载报告查看； 报告可以打印成纸质版的方便查看。 14.对平台运行软硬件环境整体监管：提供平台端系统运行监测工具，实时监测平台运行包括CPU、内存、硬件、I/O、数据交互等性能，确保管理员对平台运行健康度的掌握，降低平台运行风险。 15.分院信息系统建设：医院HIS系统以分院模式同总院HIS系统统一使用，并承担相关的费用（包括支付给HIS等厂商的接口费）。  16.远程会诊平台硬件需求：  16.1. 高清视频终端一套:一体化超高清视频会议终端，内置摄像机、阵列麦克风、高清编解码器，“双摄”设计，光学变焦可达12X，智能呈现C位视角，1080P高清，快速部署。2、配备两台55寸4K高清液晶电视。3、会议专用麦克风。  16.2. 防火墙一套:1、软硬一体产品。2、网络吞吐性能：≥1 Gbps；每秒新建连接数：≥3万；最大并发连接数：≥50万。3、标准1U机架式；内存：≥4 GB；硬盘：无；电源规格：单电源；千兆电口≥8个(含1组电口Bypass），千兆光口≥4个，不带光模块。自带3年入侵防御许可（IPS）、病毒防护许可（AV）、上网行为管理许可（AC）、SSL VPN许可并支持≥50个SSL VPN并发用户数。  16.3.计算机1台：1、CPU：≥Intel 酷睿处理器I5-12代cpu (主频3.4G 6M缓存)；2、显卡：支持两路视频输出。3、内存：≥8GB DDR3 2133；4、存储：≥1TB+256G，SATA3接口，7200rpm；5、网卡：集成10M/100/1000MB自适应网卡 ；6，≥23.8寸显示器  16.4.打印机一台：最大打印幅面A4, 黑白打印速度 28ppm ,支持自动双面打印。  16.5.高拍仪一台：拥有自然光+LED补光灯，自动对焦，500万像素，拍摄尺寸为A4尺寸系统支持CPU P4（内存512M），支持纸传真机、扫描、文档书籍实时传送  16.6.交换机一台：1、交换容量≥336Gbps，转发性能≥51Mpps；2、固化10/100/1000M以太网端口≥24，固化1G SFP光接口≥4个；3、设备MAC地址≥16K；设备采用静音无风扇节能设计  16.7.专网≥40M。 | 1 |
| 2 | 防漏费系统 | 1.医疗设备漏费控制系统，采用科学的技术方式实现对不缴费不能做检查的事前控制，不得损害医疗设备，不得增加医生的工作量。  2．系统必须有效控制缴小费做大检查（即有效控制如超声设备缴纳浅表探头的费用，实际检查心脏项目。有效控制放射设备对未缴费的部位做检查。  3．对漏费现象的控制不能采用控制打报告系统的视频源的方法，必须采用控制设备的方法，以实现事前控制  4．系统对设备必须准确识别质控和普通检查，必须有效控制利用质控做检查的现象。  5.系统必须实现自动记录每次检查的操作医生、所使用的设备、检查的患者、缴费情况、操作时间以及操作数量等。且上述记录不能在后台修改。  6.系统必须具备实时监管医疗设备的工作进程和运行状态，并保留使用记录的功能。投标文件中应具备设备状态监管实时状态显示图。  7.医疗设备必须在医院网络出现故障时，采取脱机工作，网络修复时数据回传。不但不影响被控设备正常工作，而且要能确保操作数据的精确记录。  8.系统如果采用图像识别技术进行控费，必须从医疗设备中采集原始操作视频，必须具备影像类设备违规操作视频自动上传及回放功能。不得采用外部摄像头方式，以免干扰医患隐私。  9.领导特批功能：针对需要免费检查的患者，必须通过领导审批授权后才能在终端工作站的绿色通道显示出获得授权患者的信息，此时患者才可以在终端工作站控制的设备上进行正常检查。  10.复查功能：针对需要复诊检查的患者，必须具备复查功能，系统能够存储患者信息，在有效期内仅限患者本人复查，换人检查系统可对患者进行识别（超声类检查不得采用称重床方式进行患者识别），控制检查设备，终止检查。系统可对各设备、各患者复查情况进行统计、查询。  11.应急功能：在紧急情况下，硬件部分可以支持应急功能，使医疗设备能够脱离控制，进行正常的检查工作。  12.供应商自行安排与HIS、LIS、PACS等系统的接口，并承担相关的费用（包括支付给HIS等厂商的接口费）。 | 1 |
| 3 | 终端安全管理系统 | 主机安全防护系统软件控制中心端 【部署模式】 由管理中心和客户端组成；管理中心独立部署，收集客户端信息并配置安全策略，进行后续的响应与处置；客户端软件安装在需要被管控的主机上。 【终端安全管理】 （1）支持通过统一的管理中心对多个服务器或主机进行监控； （2）支持对终端进行详细信息展示，包括网络信息、环境信息及其他信息；支持远程关闭、重启主机、修改远程管理端口等操作； （3）支持对终端上进程的运行情况进行实时监控，并可强制终止进程； （4）支持对终端上的账号信息、运行软件信息、启动项进行统计； （5）支持对终端上的CPU使用率、内存占用率、磁盘读写、上下行流量进行统计，在达到配置阈值时报警； （6）支持下发文件、安装应用程序到终端上或者远程执行命令； （7）支持对终端上的移动存储设备进行审计与管控，对默认读写权限进行控制，进行文件拷贝审计。 【风险评估与安全防护】 （1）支持查看终端漏洞扫描情况，包括但不限于操作系统漏洞、数据库漏洞、Web容器漏洞及其他组件漏洞；  （2）支持扫描后的漏洞结果报告导出；支持管理中心推送补丁到终端； （3）支持针对系统账户弱口令、应用账户弱口令进行检测； （4）支持防暴力破解，对多次登录系统失败的恶意探测IP进行锁定； （5）支持防端口扫描，对风险扫描IP进行锁定； （6）支持文件访问监控，细粒度审计文件创建、删除、写入和重命名等操作； （7）支持防违规外联，检查出站数据包，当终端连接黑名单IP时实时阻断； （8）支持绘制流量画像，展示内网所有流量和主机间通信关系，梳理通信逻辑； （9）支持渗透追踪，针对信息收集、权限提升、隧道代理、远控持久化、恶意攻击、痕迹清除等行为进行识别和阻断； （10）支持Web应用防护，包含网站漏洞防护、CC攻击防护、网站访问控制； （11）支持屏幕水印，防止通过屏幕拍照造成隐私泄露； （12）支持一键升级管理中心、客户端、病毒库、漏洞库、补丁库、Web后门库、违规外联黑名单库。 【终端防病毒】 （1）支持病毒查杀、网马查杀、勒索防御、挖矿防御； （2）支持多种压缩包、自解压包、媒体文件、加密脚本、电子邮件、邮箱文件的病毒查杀；并可进行查杀模式、多引擎设置、压缩包查杀设置等配置； （3）支持强力查杀，可对无法普通隔离的病毒文件进行强制停止进程并隔离，或动态移除到删除队列； （4）支持部分病毒感染文件的修复功能，对于二进制文件可剥离感染部分，保证应用正常使用； （5）支持及时发现并阻断勒索病毒，对于已知勒索病毒确保进程无法启动，对于未知勒索病毒确保无法加密； （6）支持发现挖矿类恶意程序，避免终端资源被非法占用。 | 1 |
| 4 | Lis、医学影像接口 | 根据设备设定（设备尚未采购）和我院现有lis及医学影像系统能进行无缝共享衔接数据，并承担相关的费用（包括支付给HIS、电子病历等厂商的接口费）。 | 1 |
|  |  |  |  |