**采购包7【具体技术（参数）要求】电子签名系统**

**1.项目背景**

近年来，在国家卫健委相关政策指导下，以电子病历为核心的医院信息化建设发展迅速，电子病历已经成为医院日常医疗服务的核心，而随着医院信息化建设的逐步推进，医院的无纸化建设也越来越受到重视。在全院推行无纸化，取消纸质病历后，能够大大减少进行手写签名的工作量，降低医护人员工作负担，同时又为医院节省了大量的纸张耗材成本。

本采购包根据医院HIS、EMR、LIS、PACS、病理、手术麻醉等医院信息系统的实际安全需求，建设医患电子签名系统，解决医院信息系统的身份认证、授权管理、责任认定等安全问题，解决电子病历的真实性、完整性、有效性等问题。基于数字证书的应用安全支撑体系，通过CA数字证书及证书应用相关产品和技术，实现电子认证服务与医院业务应用的有机结合，以满足PC端和移动端医院信息平台在身份认证、授权管理、责任认定等方面的信息安全需求，达到《电子病历系统功能应用水平分级评价方法及标准（试行）》中电子病历5级对电子签名的要求。

**2.★项目的主要内容**

| **序号** | **建设系统** | **数量** | **备注** |
| --- | --- | --- | --- |
| 1 | 协同签名系统 | 2台 |  |
| 2 | 移动端APP或SDK | 1套 |  |
| 3 | 移动个人数字证书 | 2000张 | 每张证书3年有效期，自启用日开始计算 |
| 4 | 时间戳服务器 | 2台 |  |
| 5 | 手写信息数字签名系统 | 2台 |  |
| 6 | 电子病历移动签署系统 | 1套 |  |
| 7 | 无线手写签名设备 | 50台 |  |
| 8 | 事件型证书服务 | 1项 | 3年有效使用期 |

**3.系统的实现遵循以下原则**

统一标准原则：在系统建设过程中，应“统一规范、统一代码、统一接口”。加强指导、组织和协调，规范系统的基本功能、数据模型和数据编码等信息标准。

性能稳定原则：系统应具有较强的数据处理能力，满足全院7×24小时服务的要求，保证医疗数据交换和资源共享的需要。

保证安全原则：系统运行的安全性和稳定性是业务系统正常运行的重要保障。在系统设计和建设中要符合国家有关信息安全方面的法律法规及技术要求，强化信息安全管理，制定和完善相关的应急处理预案，保证系统稳定运行。

经济实效原则：项目建设应坚持经济实效的原则，注重投入产出效益，不盲目追赶技术超前，防止大起大落，以合理的投入，产出适宜的效果。

扩展性、兼容性原则：项目的设计和实施应具有灵活的扩展能力，充分考虑国家相关标准和业务系统需求变化对数据格式、处理方式等带来的业务流程变动和模式调整。

**4.系统实施的标准要求**

系统应遵循《国家卫生信息标准基础框架》制定的统一的技术规范和相关数据共享要求。采用多层软件体系架构，以便能随时适应未来的新的需求调整，实现各级卫生部门、各业务系统的信息服务共享及各种服务的快速整合与快速响应。

系统设计和使用应确保数据的准确性、可靠性、完整性、连续性、安全性及保密性。在网络环境下，需要使用多种技术手段保护数据的安全。应符合国家及医疗卫生行业的相关信息化和数据标准或规范，如HL7 CDA、DICOM、IHE XDS、XML、ICD10、电子病历国家标准、中华人民共和国计算机信息系统安全保护条例、中华人民共和国保密法、中国计算机安全法规标准等，在大量数据环境下能保证系统的运行速度；能确保数据存储及共享的标准化。

1）优先参照国家统一标准，凡已公布国家/行业标准的遵循国家/行业标准；无国家/行业标准的参考国际标准、外国国家标准。

2）如果国家、国际没有相应标准，参考国内省市已经形成的标准、规范。

3）如果国家、国际、省市都没有相应标准，自建区标准。需自建信息字典的编制和维护，卫生信息标准的引用和参照。

**5.系统评审要求**

1. 提供的软件版本能配合采购人通过5级电子病历评审工作。
2. 具备通过6级电子病历要求的技术能力，并具备通过6级电子病历评审要求。

**6.1系统详细功能要求**

**6.1.1协同签名系统（2台）**

| **模块** | **功能** | **功能描述** |
| --- | --- | --- |
| 软件系统功能 | 基本要求 | 医护电子签名主要是指医护数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据。 |
| 证书管理 | 1）▲证书生命周期管理，包括单个/批量申请证书、单个/批量续期证书。证书下载，通过用户名、用户标识查询证书，可下载证书；证书绑定，用户标识与证书进行绑定；密码管理，包括修改密码、密码解锁（投标时需提供加盖投标人公章对应功能的产品说明书作为证明材料）。  2）证书申请，支持单个申请，一键批量申请；支持应用通过接口在线申请。  3）支持数字证书、续期、注销、变更等全生命周期服务管理，支持一键批量操作。  4）支持数字证书口令在线解锁。  5）支持证书发放数量统计。 |
| 身份认证管理 | 1）身份认证方式：通过多因子认证（口令认证、口令认证+刷脸认证、口令认证+短信认证、口令认证+指纹认证、口令认证+设备认证）、扫码认证方式进行身份认证。  2）身份认证方式管理：对认证方式进行查询、修改、添加操作。用户完成登录认证后，在一定时间内免扫码认证或免密签名，可设置免密时间长短。  3）认证提醒：第三方应用发起认证时，提醒用户进行认证确认。 |
| 授权管理 | 1）通过授权管理实现用户之间进行互相授权的操作。  2）授权用户管理：对授权用户进行查询、修改、添加授权操作。  3）申请授权：授权用户申请授权；删除授权：删除已经授权的信息；确认授权：授权人确认授权行为。  4）冻结/解冻授权：授权人可冻结授权/解冻授权。  5）授权续期：授权人可对授权用户的授权时间、授权使用次数进行续期。 |
| 电子签名管理服务 | 通过电子签名管理服务实现各场景签名应用。  1）授权签名：授权人可指定授权用户代授权人进行签名。  2）非实时签名：支持提交签名文件后，在APP上确认后才对文件进行签名。  3）协同签名：提交协同签名文件，可设置并行多人签名、多级串行签名。  4）属性选项：提交签名文件时可配置是否添加签名时间戳、内容时间戳、吊销信息（CRL信息、OCSP信息）、证书链。 |
| 电子印章 | 1）支持PDF文件电子印章功能。  2）印章管理，包括印章/个人手写签名图样采集、印章上传、印章下载。  3）▲电子签章，包括不带时间戳的签章、带时间戳的签章、指定位置签章、指定区域签章（投标时需提供加盖投标人公章对应功能的产品说明书作为证明材料）。 |
| 用户管理 | 1）对证书用户和系统管理员信息进行管理。  2）批量导入用户信息。  3）支持删除、冻结用户。 |
| 日志管理 | 1）支持管理员操作日志、接口调用日志，便于操作行为溯源。  2）支持关键操作查询和统计。 |
| 安全通信 | 移动端与服务端之间的通信全部建立在安全加密信道的基础上，确保信息传输安全。 |
| 跨平台支持 | 支持Windows、Linux、 Android/IOS移动端，微信小程序等平台。 |
| 安全性 | 1）用户密钥双重加密存储：  采用密码设备叠加用户设置的口令对用户的密钥进行加密存储，实现更安全的双重加密。  2）多因子认证：  结合用户指纹验证、用户口令进行多因子认证。  3）全面支持国产SM系列密码算法：  遵从国家密码局对签名算法的相关要求，全面支持SM2国密签名算法，同时兼容RSA等国际通用算法。  4）分组加密技术  对用户的私钥资源池进行分组，采用不同的加密密钥进行分组加密，增加密钥加密存储安全性，提高加解密效率。  5）签名私钥不出密码设备  用户在整个电子签名过程中，所有签名运算均在专用密码设备中进行，签名私钥不出密码设备，确保用户签名私钥的安全性。 |
| 签名验签服务 | 1）生成密钥：可以生成多对对称密钥（通信密钥）。由物理噪声源作为随机数，生成密钥速度快；  2）密钥存储：可以存储生成的密钥和通信密钥。密钥存储安全 ，非法者不能获得密钥；  3）数字签名：可以根据需要利用密钥对的私钥部分对信息进行数字签名。提供普通格式、PKCS#7标准的数字签名功能；  4）签名验证：提供数字签名/验证、消息签名/验证、数字信封等签名/验证功能。提供普通格式、PKCS#7标准的数字签名验证功能；  5）数字信封功能：支持封装/解封符合PKCS#7标准的数字信封；  6）证书有效性验证：提供证书有效期验证、CA根验证和CRL验证等多种验证方式和验证级别。 |
| 协同签名功能 | ▲系统基于SM2密钥分割技术和协同签名技术实现的签名，具有私钥生成、存储、使用、更新、销毁管理功能（投标时需提供加盖投标人公章对应功能的产品说明书作为证明材料）。 |
| 应用接入及授权 | 支持对接入应用的授权管理，提供restful API的形式接口与业务系统对接，产品提供对业务系统请求报文的真实性完整性校验。 |
| 签名应用 | 支持基于服务端的签名任务发起和签名结果获取；基于协同密钥技术来实现移动端用户私钥的生成和使用。 |
| 系统管理 | 支持在线、离线证书签发模式、日志及审计功能。 |
| 应用场景 | 支持一人多设备、一设备多人的应用场景；支持授权签名：用户只需要使用手机在PC端完成一次授权即可多次签名，并可以关闭授权；支持推送签名：用户以推送的方式发起签名，签名者在手机端收到推送后直接完成签名；支持在签名任务中添加签名描述信息。 |
| 支持算法 | 支持SM1、SM2、SM3、SM4等密码算法标准。 |
| 身份核验 | ▲登录时支持生物识别和手机号身份核验，验证激活码支持短信发送，短信网关可配置自建云服务短信网关和第三方短信网关（投标时需提供加盖投标人公章对应功能的产品说明书作为证明材料）。 |
| 运行状态监测 | 支持可视化管理，使用SNMP协议，系统监控、设备硬件及软件的运行状态监测功能监测数据。 |
| 统计分析 | ▲支持证书签发、签名统计、统计报表功能，按时间/证书类型/科室/姓名的查看、检索、导出功能（投标时需提供加盖投标人公章对应功能的产品说明书作为证明材料）。 |
| IPv6协议支持 | ▲产品支持IPv6协议，该功能具备《IPv6 Ready Logo认证》证书或第三方测试报告（投标时需提供证书或第三方测试报告扫描件作为证明材料）。 |
| 硬件平台配置 | 设备高度 | 2U。 |
| CPU | ≥2核，3.5GHz。 |
| 内存 | ≥2×8G。 |
| 硬盘 | ≥2×4T。 |
| 密码卡 | 内置满足密码模块安全等级第二级相关要求的密码卡。 |
| 电源 | 550W 1+1标准服务器冗余电源。 |
| 网口 | 不低于2×100/1000M自适应网口。 |
| 性能 | SM2协同签名效率≥300TPS。 |
| 系统负载 | 支持双机和集群部署。 |

**6.1.2移动端APP或SDK（1套）**

| **模块** | **功能** | **功能描述** |
| --- | --- | --- |
| 软件系统功能 | 系统兼容 | ▲移动端兼容APP（Android/IOS）、SDK、微信小程序、企业微信、钉钉小程序、H5小程序（投标时需提供加盖投标人公章对应功能的产品说明书作为证明材料）。 |
| 服务配置 | 提供服务配置功能，支持通过扫码连接服务或手动添加服务。 |
| 证书登录 | ▲提供证书登录功能，提供用户证书选择列表，支持输入证书密码进行登录（投标时需提供加盖投标人公章对应功能的产品说明书作为证明材料）。 |
| 待签列表 | 提供待签列表功能，支持展示未签名的数据列表，点击每条数据后面的“签名”即可进行单条数据的签名操作，点击该条待签数据，则可进入该数据的详情页面，也可在详情页面进行签名或者拒签的操作。 |
| 已签列表 | 提供已签列表功能，支持展示已经签完名的数据列表，点击每条数据，可进入该已签数据的详情页面。 |
| 拒签列表 | 提供拒签列表功能，支持展示拒绝签名的数据列表，点击每条数据，可进入该拒签数据的详情页面。 |
| 批量签署 | ▲提供批量签署功能，当待签数据比较多时，点击“批量签署”用户能定向选择多条数据进行批量数据签署，也可直接“全选”将所有待签数据一次性全部签署（投标时需提供加盖投标人公章对应功能的产品说明书作为证明材料）。 |
| 设置手写签章 | 提供设置手写签章功能，支持用户在移动手机上设置本人手写签章，并上传到服务端。 |
| 证书管理 | ▲提供证书管理功能，支持生物识别开关、证书密码重置、证书详情、证书删除（投标时需提供加盖投标人公章对应功能的产品说明书作为证明材料）。 |
| 自动签名管理 | ▲提供自动签名管理功能，启用自动签名，则服务端推送的自动签名数据在截止时间之前可以不经移动端签名而自动签名从而直接出现在已签页（投标时需提供加盖投标人公章对应功能的产品说明书作为证明材料）。 |

**6.1.3移动个人数字证书（2000 张）**

| **模块** | **功能** | **功能描述** |
| --- | --- | --- |
| 服务功能 | 证书用途 | 标识个人用户网络身份。 |
| 支持算法 | 签发数字证书的电子认证系统和密钥管理系统应支持国密局要求的规范算法。 |
| 证书规范 | 符合卫生部《卫生系统数字证书格式规范（试行）》。 |
| 服务规范 | 符合卫生部《卫生系统电子认证服务规范（试行）》。 |
| 证书格式 | 证书格式标准遵循x．509v3标准。 |
| 支持存放介质 | 智能USBKey、SDKEY、UimKey等。 |
| 证书拓展 | 支持自定义证书扩展域管理。 |
| 移动端密钥 | 密钥由移动终端和服务器协商产生，采用密钥分割技术保存密钥。 |

**6.1.4时间戳服务器（2台）**

| **模块** | **功能** | **功能描述** |
| --- | --- | --- |
| 软件系统功能 | 时间源服务 | 提供基于第三方精准的时间源。 |
| 时间同步 | 基于SNTP协议，从指定时间源获取标准时间并同步。 |
| 支持算法 | 支持SM2算法。 |
| TLS验证 | 支持TLS验证。 |
| 日志管理 | 提供管理日志记录。 |
| 备份恢复 | 提供备份恢复功能，保证系统瘫痪时的快速恢复。可通过界面备份当前所有配置，保证系统瘫痪时的快速恢复，支持通过证书对备份数据进行加密，通过验证证书口令解密实现备份数据恢复。 |
| 时间戳签发 | ▲支持签发可信时间戳、验证时间戳有效性，时间戳结构符合RFC3161/RFC2630/GM0033标准，支持以Adobe免集成方式签发和验证时间戳（投标时需提供加盖投标人公章对应功能的产品说明书作为证明材料）。 |
| CA配置 | ▲支持配置多CA签发根证书，对其他CA签发的时间戳采用CRL/LDAP验证方式和验证（投标时需提供加盖投标人公章对应功能的产品说明书作为证明材料）。 |
| 接口支持 | 支持多种时间戳服务接口，满足各类应用开发平台调用。 |
| 可视化管理 | 支持可视化管理，使用SNMP协议；系统监控、设备硬件及软件的运行状态监测功能。 |
| 管理员配置 | 提供分级权限管理模式，分为管理员、操作员、审计员三级，分别赋予不同权限。 |
| 支持接口 | 支持应用接口：Java、C、COM。 |
| 支持算法 | 支持SM2、SM3算法标准。 |
| 时间精度 | 授时精度0.5-3ms（毫秒），守时精度＜1ms（72小时）。 |
| 性能要求 | SM2签名≥1000次/秒，SM2验签≥500次/秒。 |
| 稳定性 | 内置恒温晶振，日老化率5E-10，秒稳定度优于2E-11，日平均准确度优于1E-12。 |
| 硬件平台配置 | 设备高度 | 2U。 |
| CPU | ≥2核，4.0GHz。 |
| 内存 | ≥2×8G。 |
| 硬盘 | ≥2×4T。 |
| 时间源模块 | 时间源模块支持4G、GPS、北斗三合一的时间源信号。 |
| 电源 | 550W 1+1标准服务器冗余电源。 |
| 网口 | 不低于2×100/1000M自适应网口。 |

**6.1.5手写信息数字签名系统（2台）**

| **模块** | **功能** | **功能描述** |
| --- | --- | --- |
| 软件系统功能 | 电子签章服务（患者签名） | 1）CA机构数字证书支持：支持第三方CA机构签发的数字证书。  2）确认文档签署者身份：通过验证签署者的数字证书是否有效来证明签署者身份的真实可靠性，并可以查看签署者身份证书，从而确认签署者。  ▲3）保护文档不被非法篡改：能对所签文档内容进行完整性认证，确定其是否被篡改。如果签署后的文档发生了变更，验证时则会提示文档验证不通过（即文档验证失败）（投标时需提供加盖投标人公章对应功能的产品说明书作为证明材料）。  4）确保文档签署者不可否认：通过数字签名的唯一性及可验证性，从而确保签署者对所签文档的不可抵赖。  5）支持PDF格式，并且印章需符合PDF的签章标准，支持Adobe Reader直接验证，无需安装任何插件。  6）支持与采购人信息系统的集成，协助应用程序厂家进行接口改造。  7）支持PDF文档批量盖章，支持坐标定位文本定位批量盖章。  8）结合电子签名、时间戳等技术为电子病案文件提供归档与长期保存解决方案，解决文件电子签名独立验证、时间链条的可追溯，电子文件保护策略等。 |
| 患者电子签名 | 1）患者电子签名主要是指患者数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据。  ▲2）支持患者电子签名（知情文书、手写签名、知情文书应用、证书签发服务、事件型证书、数据采集、数据处理、数据归档、手写签名应用）、电子签名接口改造（投标时需提供加盖投标人公章对应功能的产品说明书作为证明材料）。 |
| 知情文书签名服务 | 1）在知情文书生成后，借助外部设备对患者/家属进行身份数据采集。将采集的个人信息，如指纹信息和手写签名笔迹等，固化在PDF的知情同意书文档中。  2）文档处理，可通过手写板，抓取用户的手写笔迹形成图片，并把图片嵌入到PDF文档中。  3）电子签章和时间戳，可对PDF文档插入电子签章和时间戳。  4）支持拍照、录音，医生可根据实际需要，开启谈话录音、签署录像、拍照等功能。  5）提交，提交后系统不再可以修改，为电子归档提供基础文档数据。 |
| 终端支持 | 支持通过手写数字签名终端，获取签名人手写签字笔迹，作为数字签名可视化展现效果图示。 |
| 证书签发 | 申请和获取签名数字证书。根据签名业务及签名人鉴证信息，向电子认证服务机构证书服务平台申请颁发数字证书。 |
| 支持算法 | 支持SM2\SM3\SM4密码算法，使用SM2数字签名密码算法，对电子文书进行密码运算，保护电子文书的有效性、合法性。 |
| 证书统计 | 支持统计事件证书数量。 |
| 短信验证码签名 | 支持短信验证码签名，用户通过手机短信验证码认证方式确认签名操作，自动生成签名笔迹。 |
| 签署方式 | ▲支持一名一签，一名多签，多名多签，主要用于患者或家属在签署多份知情同意类文书签署场景（投标时提供功能截图作为证明材料）。 |
| 签名转化 | ▲CA中心根据手写数字签名系统采集和固化的可靠签署内容与行为数据，签发事件型数字证书，将手写签名转换为电子签名（投标时提供功能截图作为证明材料）。 |
| 运维监控 | 可对服务器CPU使用率、内存使用率、硬盘使用率、I/O读写等设备信息进行监控。 |
| 硬件平台配置 | 设备高度 | 2U。 |
| CPU | ≥2核，3.5GHz。 |
| 内存 | ≥2×8G。 |
| 硬盘 | ≥2×4T。 |
| 密码卡 | 内置满足密码模块安全等级第二级相关要求的密码卡。 |
| 电源 | 550W 1+1标准服务器冗余电源。 |
| 网口 | 不低于2×100/1000M自适应网口。 |
| 设备负载 | 支持双机、负载均衡。 |
| 性能指标 | 基于SM2算法手写签名效率≥108000笔/小时。 |

**6.1.6电子病历移动签署系统（1套）**

| **模块** | **功能** | **功能描述** |
| --- | --- | --- |
| 软件系统功能 | 文书管理功能 | ▲支持异常文书、待签文书、已签文书管理，支持按文书编号、所属科室、患者名称、签名模式查看各种状态的文书。 |
| 患者管理功能 | ▲支持查看患者列表，通过按科室名称、患者名称查询到患者信息。 |
| 科室管理功能 | 支持查看科室列表，支持增加、批量删除科室，按科室名称或编号查询。 |
| 安全包管理 | 支持增加、批量删除安装包，按版本号查询。 |
| 查询日志功能 | 提供查询操作日志功能，支持查看操作用户、具体操作、操作结果及操作时间。 |
| APP应用 | 支持在移动指纹手写签名屏上安装移动签署APP，获取移动签署系统中的待签文档，实现患者及家属对知情文书的签署。 |
| 数据采集 | 支持签名人身份信息、指纹、手写笔迹数据、待签署业务数据、签署时间信息等类型数据的可靠采集。 |

**6.1.7无线手写签名设备 （50台）**

| **模块** | **功能** | **功能描述** |
| --- | --- | --- |
| 软件系统功能 | 文书缓存 | ▲支持在有网络的情况缓存文书，在无网络环境下签署，并可先缓存（投标时提供功能截图作为证明材料）。 |
| 笔迹采集 | 采集签名人在LCD显示屏上的手写签名笔迹，实现签名人手写签名笔迹数据的可靠采集。 |
| 指纹采集 | 整合了指纹采集模块，可在手写签名同时记录签名人指纹数据，具有身份鉴别能力和应用安全性。 |
| 硬件配置要求 | 处理器 | CPU核心数：不低于八核，主频不低于2.8GHz。 |
| 屏幕尺寸 | 不低于10.9英寸；分辨率：不低于2560×1600。 |
| 运行内存 | 不低于6GB；内存容量：不低于128GB。 |
| 摄像头 | 前摄像头不低于800万像素，后摄像头不低于1200万像素。 |
| 触控笔 | 含原装触控笔一支，4096级主动式压力感应。 |
| 联网支持 | 网络连接支持双频WiFi，2.4G。 |
| 电池 | 聚合物高密度安全电池，电池容量标配8000mAH，电池电压7.4V，待机时长100h，工作时长8h。 |

**6.1.8事件型证书服务（1项）**

| **模块** | **功能** | **功能描述** |
| --- | --- | --- |
| 服务功能 | 身份标识 | 由CA机构为患者签发事件型数字证书，标识签名人在特定的签名事件中的数字身份。 |
| 证书内容 | 事件型数字证书除包含签发者信息、签名人信息、公钥、有效期以及一些扩展信息外，还包含本次签名事件中被签名文件的数字摘要、必要的签名人行为特征数据（例如手写签名笔迹数据），从而实现该证书与该签名人、签名文件、签名行为的可靠关联与绑定。 |
| 证书格式 | 证书格式标准遵循x．509v3标准。 |
| 私钥销毁 | 事件型数字证书的私钥在完成本次签名运算后，即时自动销毁，确保私钥仅应用于此次签名事件。 |
| 数字签名 | 事件型数字证书只针对特定签名事件中的被签名文件进行数字签名。 |

**7.项目要求**

**7.1项目技术条款**

1. 客户端系统采用CS方式则应支持以下操作系统：win10企业版32位、win10企业版64位；采用.net框架的需支持.net framework 4.5及以上。客户端采用BS方式则应支持：WIN10以上操作系统调用操作系统默认edge浏览器。
2. 整个系统从客户端、中间层、数据库层支持虚拟化技术，可在虚拟化环境下正常运行，支持vm等常见的虚拟机。
3. 网络安全等保要求：中标人应根据公安机关的时间要求无条件对本采购包中所涉及的设备及系统进行安全漏洞检测和修复，并配合采购人完成日常等级保护检测和漏洞修复工作，以满足通过等级保护验收的要求。根据采购人提供的方案进行整改。系统整体安全级别需完全符合国家《网络安全等级保护2.0》三级标准的相关要求。如网络扫描发现高危、中危漏洞需通知相关责任人立即修复，并需出一份系统安全整改报告盖中标人的公章。
4. 商用密码要求：按照国家相关商用密码应用和管理要求，配合相关部门的要求完成商用密码评估及整改工作。
5. 应用服务器与数据库服务器（含数据文件）分离，分别部署在不同的服务器上。
6. 项目验收前中标人完成所有与该系统有关的信息系统、政策性任务、医疗设备等接口开发调试工作，并保证接口的正常运行投入使用。
7. 服务器操作系统相关：优先采用Linux操作系统及配套成熟组件部署业务系统再考虑采用Windows Server 2016操作系统及配套成熟组件部署业务系统，并自带序列号激活码。
8. 如系统牵涉财务收费对账问题，则需有相关的对账报表以辅助业务科室完成对账工作。
9. 本采购包实现的成果，配合采购人进行成果转化，申请软件著作权等。

**7.2项目实施要求**

1）本采购包在合同履行期限内中标人需投入团队人员至少2名（其中包括驻场人员至少2名）。

2）驻场人员驻场期间在采购人办公室办公，并每天向主管工程师手写签到，正常上班期间按医院作息时间执行。

3）中标人应在签订合同后15天内到采购人指定地点完成如下事项：成立项目组织，有项目实施方案、项目进度甘特图，WBS工作详细分解包、确定与其他系统的接口。在项目实施过程中与其他系统的接口先行，并能按计划推进项目，按时按质完成工作。

4）中标人每周提交一次项目周报。

5）中标人负责系统的安装部署、调试并能正常运行。

6）系统运行所需的各种环境安装包由中标人提供并负责安装。

7）中标人应在本采购包中负责提供“软件”，并提供安装调试、培训和售后技术支持服务，所提供软件保证满足采购人功能要求，数据准确、速度快捷、运行稳定，保证系统的正常应用。

8）中标人应能熟练操作及应用全部系统，确保采购人相关业务人员对其使用的应用系统能熟练操作使用。

9）中标人接受监理单位对项目监督管理的相关条款。

10）本采购包建设全生命周期工作中标人需派遣中标人公司自有员工负责该部分系统调研、开发、测试、安装调试、培训、上线保障、售后服务等。