01 包采购需求

1、项目概况

1.1 项目建设背景

2020 年 3 月,《安徽省人民政府关于 2020 年实施 33 项民生工程的通知》(皖政办〔2020〕17 号）新增了“智慧健康建设”工程，明确提出，围绕《健康中国行动（2019-2030）》和新冠肺炎疫情防控新形势，在继续推进“智医助理”基础上，加快“智联网医院”建设，面向基层打造人机协同的诊疗模式，提升基层医疗服务水平。

“智联网医院”项目与“智医助理”项目是安徽省贯彻“强基层”国家战略的创新，是安徽省发展智慧健康、提升基层医疗服务水平的两大重要举措。

在人工智能辅助诊断方面，通过“智医助理”在基层医生诊断过程探索人工智能技术的应用与落地。“智医助理”自 2018 年于四县一区开展试点，经过近三年的建设，已在全省 16 个地级市的所有基层医疗卫生机构全覆盖。通过“辅助诊断”功能，提升基层医生的对常见病、多发病的诊断准确性，实现我省基层诊断合理性从 77%到 88%的提升；通过“病历质控”功能，提升基层病历的质量，实现我省基层病历规范率从 20%到 95%的大跨越；通过“诊断监管”业务，使我省在全国率先实现全省所有基层医疗服务信息以统一数据模型、统一标准汇集至省级平台。

在人机协同治疗审核与专家协作方面，“智联网医院”将通过汇聚区域内等级医院的专家资源与人工智能技术，一起构建人机协同模式。将于 2020 年在合肥市、宿州市、池州市的 18 个县（市、区）开展项目试点。通过治疗适宜性审核功能，可有效辅助基层医生在明确诊断后开展治疗服务，提升用药与处置的合理性；通过汇聚区域内等级医院专家资源，为基层医生在诊疗过程提供医学专家指导与协助，进一步降低漏诊、误诊，提升基层诊断合理率；通过诊疗服务监管功能，可构建我省面向基层，诊断与治疗全流程的业务监管体系。

本试点项目的建设，是在遵循国家与安徽省关于利用新型技术手段赋能基层诊疗相关政策指引的基础上，我省在医疗业务层面开展的新探索，是建立提升基层医疗服务质量的新手段，也是安徽省继“智医助理”在全国取得标杆示范之后的又一创新，是安徽省在全国率先打造“智慧医疗体系”的主要系统之一，更是安徽省在全国率先面向基层打造人机协同诊疗模式，提升基层医疗服务水平的创新举措。项目建设政策依据充分、业务需求可达、技术落地较成熟。

1.2 项目建设目标

“智联网医院”向下对接安徽省基层医疗卫生机构，向上对接各地市试点医院，并通过“智联网医院”平台构建的人工智能基础能力、标准化医学知识共享能力、诊疗风险自动检测评估能力，促进诊疗资源精准对接、高效医疗服务、政府科学决策，推进区域构建高效医疗卫生服务体系，助力安徽省在全国率先构建面向基层的人机协同诊疗模式，具体实现以下几个核心目标：

（1）通过构建治疗适宜性审核体系，降低基层医生治疗风险；

（2）通过构建人机协同诊断模式，提升基层鉴别诊断能力；

（3）通过构建病例风险分级体系，确保专家资源切实可配；

（4）通过构建业务监管统计体系，实现创新业务可管可控。

1.3 项目建设任务

依据安徽省2020年民生工程关于“智慧健康建设”的总体规划，本项目将充分利用安徽省“智医助理”在基层大规模常态化应用的优势，建设集治疗适宜性审核、诊疗风险评估、上级专家审核、转诊辅助、患者应用、监管统计、基础管理等服务为一体的安徽省“智联网医院”，覆盖试点医院以及基层医疗卫生机构，具体包括：

（1）建设核心能力平台，为“智联网医院”各业务应用提供人工智能能力支撑。

（2）建设信息支撑平台，为“智联网医院”各业务应用提供核心数据与业务保障。

（3）建设业务应用系统，在全国率先面向基层打造人机协同诊疗模式，提升基层医疗服务水平。

1.4 服务范围

本项目需要针对采购人提出的业务功能需求，定制开发对应的应用软件系统，并配套完成软硬件设备的系统集成。建设核心能力平台、信息支撑平台、治疗适宜性审核子系统、风险诊疗病例评估子系统、专家审核子系统、转诊辅助子系统、患者应用子系统、监管统计子系统、监管统计子系统、基础管理子系统。

安徽省“智联网医院”覆盖合肥市、宿州市、池州市地区试点医院以及基层医疗卫生机构，具体建设范围如下：

（1）“智联网医院”上游覆盖合肥市、宿州市、池州市共计35家试点医院，上游医院主要提供医生专家与其他诊疗资源，实现风险审核与转诊辅助等业务，预估上级医疗机构专家用户数量为1500人。试点医院名单如下：

地点	试点医院
合肥市	中国科技大学附属第一医院（安徽省立医院）、合肥市第一人民医院、合肥市第二人民医院、合肥市第三人民医院、合肥市滨湖医院、肥东县人民医院、肥东县中医医院、肥西县人民医院、肥西县中医院、长丰县人民医院、长丰县中医院、庐江县人民医院、庐江县中医院
宿州市	宿州市第一人民医院、宿州市第三人民医院、宿州市立医院、埇桥区中医院、宿州市中医院、砀山县人民医院、砀山县中医院、萧县人民医院、萧县中医院、灵璧县人民医院、灵璧县中医院、泗县人民医院、泗县中医院
池州市	池州市人民医院、池州市第二人民医院、池州市中医院、东至县人民医院、东至县中医院、青阳县人民医院、青阳县中医院、石台县人民医院、石台县中医院

（2）“智联网医院”下游覆盖合肥市、宿州市、池州市共计3832家基层医疗卫生机构，预估基层医生用户数量为7500人（因基层机构动态调整，具体机构数以项目实施为准）。

1.5 项目工期要求

自签订合同之日起，180个日历天内建设完成。

2 软件开发需求

2.1 总体设计要求

2.1.1 总体框架要求

基于安徽省卫生健康委计算中心云平台统一提供的计算资源、存储资源、网络资源、安全资源等各项云基础设施，为上层应用提供基础设施支撑。

（一）数据层

数据层通过对数据中心内数据进行深入分析、挖掘处理，形成数据层立体资源库。纵向与各级卫生健康信息系统数据同步和交换，横向与对接的各级医疗机构数据进行交换，同时通过 web 服务等形式提供统一服务，为具体业务场景提供数据能力服务。包括基础数据、索引数据、业务数据、分析数据库等。

（二）能力层

通过对核心服务的封装为上层业务提供能力支撑。根据本项目业务需要，核心能力平台在成品组件与引擎工具的基础上（包括医学挖掘引擎、医学分词能力组件、疾病术语标准化能力组件、医学同义词推荐引擎、语义理解引擎、语音识别引擎、OCR 识别能力引擎），构建人工智能基础能力、标准化医学知识共享能力、诊疗风险自动监测评估能力三大类基础能力，为前端服务与业务应用提供能力支撑。

（三）服务层

服务层主要提供技术架构中要求的平台即服务能力。安徽省“智联网医院”试点项目通过构建服务于“智联网医院”的信息支撑云平台，在成品组件与引擎工具的基础上（包括分布式定时调度组件、多模态分布式消息队列引擎、数据交换引擎、图文存储检索组件、系统运行监测组件等），实现平台服务（Platform-as-a-Service，PAAS）能力，具体包括数据访问权限控制模块、基于消息队列的数据处理模块、医学信息模型化转化模块、医疗数据文档化存储模块、医疗对象索引标识化模块、结构化数据交换模块、数据脱敏模块、数据加密模块、消息提醒服务。

（四）业务层

业务层基于服务层提供的能力，向患者及接入的各级医疗卫生机构提供相关应用。主要包括治疗适宜性审核、风险诊疗病例评估、专家审核、转诊辅助、患者应用、监管统计、基础管理等应用。覆盖了卫生健康主管单位、各级医疗机构、医生等医疗健康服务主体，实现了提升基层鉴别诊断能力、降低基层诊疗用药风险、提升基层实际诊治效果等多方位的智能应用系统。

2.1.2 应用架构需求

安徽省“智联网医院”试点项目建设采用省级统筹建设，这种模式下，可确保相关信息系统具备足够高的安全性、健壮性。总体应用架构采用统一规划原则，面向省级医院、市级医院、县级医院、基层医疗卫生机构、医生以及医疗机构运营人员、卫生部门管理者提供相应的智能应用。

通过构建服务“智联网医院”的信息支撑平台，建立上级医疗机构与基层医疗卫生机构的对口联系机制，实现与“智医助理”系统互联互通，打造基层诊疗管理闭环，帮助基层医疗卫生机构筛选诊断与治疗信息。对高风险病例审核及干预，降低基层医疗卫生机构误诊漏诊率，提升基层鉴别诊断能力，降低基层诊疗用药风险，提升基层实际诊治效果，助力安徽省在全国率先构建面向基层的人机协同诊疗模式。

2.1.3 数据架构需求

安徽省“智联网医院”数据架构的整体设计理念是建立“智联网医院”信息模型框架，统一医疗卫生业务数据各环节的语义和认知，指导信息系统数据模型标准和系统间交互标准规范的建立；建立领域数据服务模型和分析决策模型，为上层应用提供安全、一致的数据访问和数据分析服务，为“智联网医院”业务的开展提供技术支持。

2.1.4 逻辑部署需求

“智联网医院”平台部署在安徽省卫生健康委中心机房。“智联网医院”需要访问各试点地市“智医助理”能力平台中的数据，需要与各市“智医助理”能力平台进行网络互通，进行数据传输。现各试点地市均已建立从市到省中心的完整网络体系，所以将“智联网医院”平台部署在安徽省卫生健康委信息中心既可以为提供网络保证，又可以节约网络建设成本。

2.1.5 性能指标需求

（1）稳定性指标

整个系统能够连续 7×24 小时不间断工作。系统运行每 1000 小时中可用时间至少不小于 999 小时，故障间隔时间应大于 1000 小时。系统保证数据的一致性，完整性，准确性要求达到 99.99%。对客户输入的数据进行合法性检查，确保流程的通畅性，并且能够对错误数据进行自动纠错处理。

（2）系统响应时间指标

提供多种优化设计方法和多种运行模式，尽可能降低服务器端负载和用户操作响应时间。服务器端需要综合考虑数据量、用户量、并发访问量、数据和应用服务的提供模式，采用能满足系统稳定高效运行所需的服务器、负载均衡设备、高性能的系统基础软件等。

一般性操作最长不超过 2 秒，对一般性统计不超过 60 秒。当操作员做一些处理时间较长的操作时，在界面上能给出提示信息。在返回数据量过大导致响应时间过长时，能提供部分响应，例如分页取数据等，减少等待的时间。

2.2 应用支撑平台与应用系统建设需求

2.2.1 核心能力平台建设需求

核心能力平台为位于系统的能力层，通过对核心服务的封装为上层业务提供能力支撑。根据本项目业务需要，核心能力平台包括以下内容：

2.2.1.1 医学数据结构化能力

医学文本结构化处理能力，对电子病历、住院病历等医学文本抽取其中的医学要素，如症状、体征、疾病等，结构化后的数据可用于人工智能使用。主要包括：

（1）医学实体信息抽取。识别文本中的生物医学实体，如病历中的诊断名称、姓名、年龄、检查项等，药品说明书中的名称、剂量、时间溶媒等，其目的在于通过识别医学关键概念并可以进一步提取关系和其他信息，并将识别的医学概念，如疾病，使用疾病术语标准化能力组件，以标准化的形式（医学术语）表示出来。

（2）实体间关系抽取。识别文本中实体与实体之间的关系，医学领域相对专业封闭，其实体类型可枚举（如疾病、病原体、药品、特殊人群等），因此实体之间的关系也是有限的可枚举的，可通过预定义实体与实体之间的关系，将抽取任务转换成分类任务来解决。如抽取病历中病原体与疾病之间的关系、疾病与手术之间的关系、症状与属性之间的关系、药物与病原体之间的关系。

（3）属性抽取。属性抽取是指对属性和属性值对的抽取，属性值的抽取是指从文本中抽取实体附加属性的属性值，医疗文本中存在大量的描述实体属性的信息，属性抽取的技术

方案和关系抽取比较类似，不同的是，关系是反映实体外部的联系，而属性则是实体的内部特征。例如，“皮肤”是一个身体部位实体，“红”、“肿胀”、“瘙痒”都可以是其属性。

系统应支持基层、二级、三级医院的门诊病历的结构化理解；覆盖疾病、症状等 30+种标签及相互关系提取。

2.2.1.2 基于知识图谱的知识推理能力

基于构建的知识图谱，提供基础的知识推理能力，即帮助由 A 到 B 的推理，可用于治疗适宜性审核。

依托医学认知智能技术和医学知识体系，模拟医生看病的整个过程，随着问诊过程的不断推进，可以获取到的病人相关信息不断增强，系统对病人的病情也会更加了解，系统会根据病人不同阶段的病情，给出不同的判断，并随着信息的增加，最终给出更加精确的推荐结果。同时针对初诊、复诊等不同的诊疗场景，也会根据不同治疗恢复的不同阶段的身体状况，给出合理的病情判断。

支持门诊质检细则近百种，覆盖安徽地区门诊病历质量评定标准。

通过自动化审核，协助药师审方，大幅提升审核效率，对不合理用药行为进行规避。系统具备业务可扩展能力，可根据需要增加新的业务规则，支持知识推理能力。

2.2.1.3 基于深度学习的医学语义度量能力

具备文本相似度度量能力，如可用于通过计算电子病历的相似度，在做治疗适宜性和风险检测时，可通过对历史数据的应用进行适宜性和风险检测。

统计模型重在从海量医学数据库中通过语义度量获得最相似的数据，语义表示是否精确会直接影响病情获取的准确率，在统计模型中的语义表示层面，需采用多信息融合的语义表示及度量方法。

支持业务分类效果，准确率应达到 95%以上。

2.2.1.4 基于深层次语义理解的医学检索知识服务

具备医学知识检索能力，用户可检索电子病历、医学指南、科学文献等，在本项目主要做药品的检测，该组件可供用户和其他模块共同使用。

支持电子病历、医学指南、科学文献、医学教科书内容检索，准确率 90%以上。

2.2.1.5 面向用户的结构化知识问答展示服务

具备医学知识问答能力，用户可直接向系统提出医学方面的问题，系统直接返回问题的答案。采用权威医学知识内容供医生使用，支持疾病知识库、药品知识库、检查检验、健康知识、中医、临床路径、诊疗规范及指南等知识库，查准率 90%以上，查全率 85%以上。

2.2.1.6 面向业务应用的推理知识共享服务

具备面向具体业务应用场景的知识推理能力，支持诊断推荐、病历检查等。

支持国家卫生健康委“优质服务基层行”66 种疾病，支持“乡镇卫生院/社区卫生服务中心服务能力评价指南”129 种基本病种，扩展到基层常见病种、多发病 3000+；危急重病/症 200+。

支持门诊质检细则近百种，覆盖安徽地区门诊病历质量评定标准。

协助药师审方，通过自动化审核，效率提升 50%以上，对不合理用药行为进行规避，采纳率达到 85%以上。

2.2.1.7 高风险症状识别监测能力

具备高风险症状识别能力，辅助医生识别患者的高风险症状并发出预警。

2.2.1.8 风险诊断识别检测能力

具备高风险疾病识别能力，辅助医生识别患者的高风险疾病并发出预警。

2.2.1.9 治疗适宜性识别监测能力

具备治疗方案适宜性评估能力，包括方案推荐、方案审核，辅助医生出具合理的治疗方案，并对方案中的风险进行预警。

支持从药物遴选、用药指征、给药剂量、给药途径、用药疗程、给药频次、联合用药、溶媒选择、溶媒剂量、禁忌、重复用药等维度对医嘱进行审核。

2.2.1.10 诊疗效果监测评估能力

具备治疗效果评估能力，辅助医生对患者的治疗效果进行评估，医生可根据评估结果调整治疗方案。系统参照县级医院与乡镇卫生院能力评价标准与应治应收疾病目录，同时学习 CMI 评价标准，从而构建完成能力体系。

系统应用过程中应综合考虑医院收治患者的结构和疑难度，对患者的病种、病情、年龄、性别、阳性体征等因素进行量化分析，从而实现对患者的诊疗风险等级的评估，患者的风险等级不同，后续匹配的医生也不同。

2.2.2 信息支撑平台建设需求

信息支撑平台是整体智联网医院系统建设的重要技术平台支撑，用以提供给上层子系统集成调用。主要包括数据访问权限控制模块、数据脱敏模块、数据加密模块、结构化数据交换模块、医疗信息模型化转换模块、医疗数据文档化存储模块、医疗对象素引标识化模块、基于消息队列的数据处理模块、消息提醒服务。

2.2.2.1 数据访问权限控制模块

数据访问权限控制模块主要实现对于不同系统交互、用户对象使用时，对数据记录使用权限控制。通过在后台将数据有机的先行划分与整合，按照事件逻辑自定义数据权限，配合基础管理子系统以实现在系统交互过程中，用户使用过程中的各项数据权限控制，能更灵活、更深层次的配置业务过程数据操作权限及数据可见权限，全面保障数据的安全性。

2.2.2.2 数据脱敏模块

数据脱敏模块是对某些敏感信息通过脱敏规则进行数据的变形，实现敏感隐私数据的可靠保护。在涉及患者安全数据或者一些商业性敏感数据的情况下，在不违反系统规则条件下，对真实数据进行改造并提供测试使用，如姓名、身份证号、手机号、就诊卡号、住址等信息都需要进行数据脱敏。“智联网医院”系统中提供随机值替换脱敏和特殊字符替换脱敏两种脱敏方式，并在动态和静态场景下均提供对应的数据脱敏功能。

2.2.2.3 数据加密模块

“智联网医院”项目建设过程中，为保障数据的安全、准确性，中标方需与各对接厂商商定使用国产加密算法对各系统之间传输的数据进行加密，保障传输过程中数据的安全性。在数据存储过程中使用国产加密算法，对医生、患者个人敏感数据进行存储加密，保障数据存储过程安全。

2.2.2.4 结构化数据交换模块

在整个医疗信息化系统中，由于开发时间或开发部门的不同，往往有多个异构的、运行在不同的软硬件平台上的信息系统同时运行，这些系统的数据源彼此独立、相互封闭，使得数据难以在系统之间交流、共享和融合，从而形成了"信息孤岛"。随着信息化应用的不断

深入，内部与外部信息交互的需求日益强烈，急切需要对已有的信息进行整合，联通“信息孤岛”，共享信息。

2.2.2.5 医疗信息模型化转换模块

智联网医疗平台连接的是等级医院和基层医疗机构，对于不同机构的患者基本信息、临床病历数据等，由于不同系统的信息模型存在差异，主要表现在数据标准中的数据元、值域等存在不一致，同时在字段的饱和度方面有不同，所以需要进行信息模型的转化和填充。

2.2.2.6 医疗数据文档化存储模块

“智联网医院”除了大量的机构化数据需要存储使用之外，还含有大量非结构化数据如：原始病历、语音、医学影像、视频等。医疗数据文档化存储模块目的在于满足“智联网医院”在内容存储能力方面的需求，主要针对大小对象定制了不同的存储策略以提高存储能力；在随后的运营和需求收集分析过程中，提取了公共诉求，打造了提供高效、稳定的统一对象存储中间件。旨在降低团队的开发成本，提供更好的对象存储能力支撑。进而有效地降低了开发人员门槛，为接入产品在存储方面的质量提供了保证。

2.2.2.7 医疗对象素引标识化模块

智联网医院的数据模型当中，需要针对患者、机构、药品等建立主数据模型，并对于这些对象模型建立索引标识，实现这些对象的合并，增加和修改。

2.2.2.8 基于消息队列的数据处理模块

项目采用多模态分布式消息队列引擎，构建基于消息队列的数据处理模块，可支持多种消息转发、交换、适配、存储，帮助应用解决分布式系统间传递数据、通知消息，构建松耦合系统。

2.2.2.9 消息提醒服务

该服务依据用户的需求主动推送通知消息，最终用户可在短信、电话、电子邮件、应用、APP、微信公众号等终端进行接收。建立系统应用和移动设备之间联系，为各系统功能模块提高可靠的、可扩展、海量的信息提醒服务。

2.2.3 应用系统建设需求

2.2.3.1 治疗适宜性审核子系统建设需求

本项目建设治疗适宜性审核子系统，主要用户对象为基层医生。

系统通过对接“智医助理”系统，获取到基层医生在当前诊疗过程中产生的业务数据，通过将当前诊疗数据和系统收集到的既往信息数据与核心能力平台进行交互，对医生诊疗过程中容易出现的治疗适宜性风险进行监测、提醒、管理等。治疗适宜性审核子系统通过调用治疗适宜性审核能力模型，基于医学认知智能技术和医学知识体系，针对治疗的适宜性进行分析并能开展常见治疗风险问题的监测，例如人群适应性、脏器功能适宜性、适应证、禁忌证、药物相互作用、配伍禁忌以及用法用量的监测，并能在基层医生诊疗过程中需提供用药审核、方案建议等服务，对治疗不适宜的情况进行及时提醒。能实现依托基层实际情况，给与医生推荐适宜用药，辅助医生制定诊疗方案等功能。

在整个诊疗过程中，系统需在以下场景发挥作用，首先需要对患者健康档案、既往史病史进行摘要抽取；其次需要对患者结构化病历的关键信息进行抽取；最后对处方内容进行抽取，开展处方规则的论证。最终，系统会通过人工智能技术对治疗适宜性进行评估，针对无风险病例，不需提醒；针对有风险的病例，需要进行提醒。同时为了给医生更全面的建议，

项目设计的信息化系统还需要对治疗不适宜信息展示、不合理原因告知以及治疗适宜性建议和推荐。

功能模块要求如下：

2.2.3.1.1 基于相似认知的数据映射管理模块

对药物、药品、处置数据进行智能映射匹配，并提升关联效率。主要包括基础数据字典管理、药品信息管理模块、药物目录模糊识别模块、机构处置目录模糊识别模块、机构药品目录模糊识别模块、映射数据审核模块。

2.2.3.1.2 治疗适宜性规则管理模块

基层医生在诊疗过程中可能会出现不同类型的风险情况，面对不同的情况在前端用户展示时，需要有不同的展现机制，以更为友好的交互方式帮助基层医生。主要包括治疗方案宜用规则参数化管理、治疗方案慎用规则参数化管理、治疗方案禁用规则参数化管理、用法用量参数化管理、治疗方案组合规则参数化管理。

2.2.3.1.3 治疗适宜性监测告警模块

主要包括慎用药品告警提示、药品禁忌告警提示、给药剂量分析告警提示、给药频次分析告警提示、药物遴选分析告警提示、无用药指征判断告警提示、给药途径分析告警提示、超疗程用药判断告警提示、联合用药分析告警提示、溶媒选择分析告警提示。

2.2.3.1.4 基于病情数据的专家咨询

专家问题咨询功能支持医生在诊疗过程中遇到问题或对专家审核意见存在疑问可快速提交至专家处进行解答，支持基层医生通过文字内容对遇到的问题或知识点进行描述。主要包括患者病情摘要辅助模块、病历信息智能截屏模块、医学知识关联推荐模块、即时问询交互模块。

2.2.3.1.5 记录管理中心

主要包括消息列表、处理状态动态展示、历次交互详情展示、多维数据筛选、消息提醒模式设置等功能。

2.2.3.2 风险诊疗病例评估子系统建设需求

本项目建设风险诊疗病例评估子系统。风险诊疗病例评估子系统的主要用户对象为基层医生。

系统通过对接“智医助理”系统，获取到基层医生在当前诊疗过程中产生的业务数据，通过将当前诊疗数据和系统收集到的既往信息数据与核心能力平台进行交互，获取到核心能力平台反馈的风险判断结果，包括“智医助理”诊断不一致、异常复诊行为、高风险用药等判断结果，如出现风险项，则在诊疗过程中需要及时给与医生提醒，便于医生进行及时关注与修改。

当诊疗完成后，会再次对于数据内容进行分析，对于仍存在风险的病历再划分不同风险等级，并提交给上级医生进行审核。

功能模块要求如下：

2.2.3.2.1 面向多系统业务调用的支持模块

主要包括医疗数据消息队列处理、医疗数据文档存储查询。

2.2.3.2.2 风险诊疗病例评分模块

收集试点各地市基层医疗机构健康档案数据与病历数据，完成权重与算法的分析预设，进行风险诊疗病历评分模块设计。主要包括健康危害因素综合评分、误诊综合评分、危急重症综合评分、患者治疗效果评分。

2.2.3.2.3 基于 RW 值测算的病情综合评估

DRG 权重（RW）是指根据医疗费用越高消耗的资源越多，病情相对越严重的总体思路，计算每个 DRGs 组相对全省次均费用的权重，综合反映各 DRG 组的疾病严重程度和资源消耗情况。项目实施过程中需要在设计阶段收集试点各地市基层医疗机构诊断与医疗费用消耗数据，完成权重与算法的分析预设。

2.2.3.2.4 风险内容等级评估特异性配置

系统实际过程中可能面临不同地区的特异性问题，需要能按区域对风险内容进行特异性配置，实现不同区域不同的参数配置。

2.2.3.2.5 风险等级证据可视化指示

对于系统发现的风险因子需要能可视化进行展示，展示的形式包含证据知识图谱和证据来源展示。

2.2.3.3 专家审核子系统建设需求

本项目建设专家审核子系统，该系统的主要用户对象为县级、市级、省级医院的专家医生，实现上级专家对风险病例的审核和医生咨询问题的指导。

当系统发现风险病例后或有基层医生提出问题后，相应的数据均会进入“专家审核子系统”。由不同层级的上级医生进行审核与指导。首先，在县域医共体下，基层医生遇到相应问题，首先提交至县级医院医生层面，如能解决问题，则会形成审核结论以及提醒下达给基层医生，并对基层医生开展疑问解答。

其次，在县级医院医生层面，碰到难以判断的疑难问题，可继续提交至市级、省级医院专家（具体上下级间的管理关系依据实际情况而定，系统提供向上转办的功能）。同时若系统判断某一病例的风险程度极高，也会直接推送给省级医院专家。专家形成审核结论以及提醒下达给基层医生，同时转办该问题的县级或市级医生，同样可查看来自高层级专家的审核与指导意见。

该系统包含上级医生的网页端和手机移动端两个入口。

系统对于风险的分级标准，需参照相应疾病推荐指南、临床应用教材、国家相应的疾病诊治目录、标准与规范等，做到有据可依，智能实现。

功能模块要求如下：

2.2.3.3.1 多模态融合交互引擎

主要包括多模态交互消息检测组件、交互式消息动态融合组件、交互消息异常处理组件、交互消息样式匹配组件。

2.2.3.3.2 统一任务服务

主要包括问询任务调度、审核任务调度、多任务分流。

2.2.3.3.3 基于 BS 架构的专家审核网页端

主要包括审核任务统一管理、病历内容自动提取与多维展示、专家指导信息交互模块、专家工作量统计分析。

2.2.3.3.4 基于安卓架构的专家审核移动端

主要包括审核任务统一管理、病历内容自动提取与多维展示、专家指导信息交互模块、语音辅助输入。

2.2.3.4 转诊辅助子系统建设需求

本项目建设转诊辅助子系统，本系统对下联通各基层医疗机构，能获取患者的身份信息、诊疗信息，对上联通试点等级医院。用户对象包含基层医生、上级医院运营人员、上级医院临床医生。

系统通过对接“智医助理”系统，获取到基层医生在当前诊疗过程中产生的业务数据，当基层机构遇到实施救治的病例或受诊疗条件限制不能诊治的疑难复杂病历、疾病诊治超出本机构核准诊疗科目的病例时，可进行患者的上转。当上级医院中的患者在病情稳定后或是遇到需长期康复治疗的慢性病人、各种恶性肿瘤病人的晚期非手术治疗和临终关怀、自愿要求转回基层医疗卫生机构并适宜基层后续治疗或康复者，上级医生可执行下转操作。系统通过对接能帮助转出医生更少的进行信息录入，接收的医生更多的查阅信息内容。

功能模块要求如下：

2.2.3.4.1 转诊资源与关系配置管理

针对转诊机构、转诊关系、资源登记等情况进行综合管理，主要包括多级转诊关系配置、基于库存管理的机构资源配置。

2.2.3.4.2 转诊条件管理

主要包括上转条件参数化管理、下转条件参数化管理。

2.2.3.4.3 机构与资源质量评估

对各机构水平和资源质量按多维度进行评分。

2.2.3.4.4 适宜资源智能推荐

包括转诊资源选择、资源智能调度、转诊资源可视化等。

2.2.3.4.5 转诊发起端

主要包括基于智医助理的基层医生转诊、基于 B/S 架构的上级医生转诊、转诊信息辅助生成与智能引入。

2.2.3.4.6 转诊审批端

主要包括转诊信息综合管理、转诊任务分配。

2.2.3.4.7 转诊接收端

主要包括接收患者管理综合、患者信息详情调阅。

2.2.3.5 患者应用子系统建设需求

本项目建设患者应用子系统，主要用户对象为通过智联网医院项目进行转诊工作的用户，通过 H5 网页形式对居民进行服务，支持患者通过皖事通 APP 等形式进行账号注册、登录等。登录完成后，患者可进行个人信息绑定工作，便于完成用户身份对应工作。同时支持支持患者通过系统调用自己的电子健康卡，进行身份验证、服务登记等各项业务内容的开展。居民还能通过该系统对当前的诊疗服务进度进行跟踪，完成服务后对服务质量进行评价。同时为便于系统推广与使用，后续该系统还可与省内“皖事通”等相关系统进行对接与挂载，进一步便于广大居民使用。

功能模块要求如下：

2.2.3.5.1 患者信息自助模块

包括用户登录与用户绑定

2.2.3.5.2 电子健康卡调用

支持患者通过系统调用自己的电子健康卡，进行身份验证、服务登记等各项业务内容的开展。

2.2.3.5.3 服务进度跟踪管理

包括流程查询与流程详情查看。

2.2.3.5.4 服务评价模块

当患者完成服务后，支持患者对服务内容进行评价，包括但不限于资源质量、服务态度的评价。

2.2.3.6 监管统计子系统建设需求

本项目建设监管统计子系统，系统需要进行数据元管理，并通过数据治理、数据集成、监管业务建模，实现各类业务开展情况的可视化监管呈现，并提供项目运行管理驾驶舱等功能模块。

功能模块要求如下：

2.2.3.6.1 数据元管理

数据元管理为业务方提供元数据新增、编辑、维护的功能，用于业务方标准化管理本业务相关的字段，用于后期数据的统一管理。主要包括业务信息源管理、业务信息元数据管理。

2.2.3.6.2 数据集成

数据集成模块作为底层基础支撑性服务，是大数据系统的基础组成部分。主要包括数据结构转换模块、集成任务调度管理、集成状态监测模块。

2.2.3.6.3 数据治理模块

数据治理模块能发现问题数据、清洗转换数据，实现达到规范数据的生成、持续改进数据质量、最大化数据价值的目的。主要包括数据质量验证、数据清洗、数据槽填。

2.2.3.6.4 监管业务建模

数据建模支持按照业务领域对现在数据中心的数据进行整合、配置模型中数据计算规则，再通过调度平台进行任务调度，后台计算引擎生成新的数据资源，为上层应用提供数据支撑。主要包括监管指标分类管理、监管指标参数管理、监管指标组合管理、指标脚本动态调度。

2.2.3.6.5 监管可视化呈现

根据监管指标的性质、用途等特性对监管指标进行分类管理。主要包括治疗适宜性审核业务监管可视化、风险分级业务监管可视化、基层医生问询业务监管可视化、专家风险审核业务监管可视化、专家咨询指导业务监管可视化、转诊业务监管可视化、专家资源分布可视化、风险病历分布可视化、系统运行状态可视化。

2.2.3.6.6 项目运行管理驾驶舱

帮助主管部门在做决策时，提供所需要的数据以及预警的重要基础支撑。主要包括运行规则监管、运行业务量监管、告警业务量监管。

2.2.3.7 基础管理子系统建设需求

本项目建设基础管理子系统。基础管理子系统需要面向参与“智联网医院”的机构与部门管理人员使用，支持“智联网医院”注册与登录机构管理、人员账号管理、功能与数据权限调整，保障“智联网医院”后台的有效运营和维护，支撑前端人员更好的使用。

功能模块要求如下：

2.2.3.7.1 医疗机构管理

包括机构新建、机构信息管理、批量机构导入、机构信息调阅

2.2.3.7.2 临床学科管理

包括学科新建、标准化信息管理、学科能力水平评价。

2.2.3.7.3 专家资源管理

包括专家库管理、专家详细信息登记、标准化信息管理、服务信息配置、专家信息调阅。

2.2.3.7.4 服务资质认证管理

对于参与“智联网医院”的医疗机构及专业医疗人员，需要进行资质认证，包含认证信息填写、部分图片内容上传、查看审核进度等。

2.2.3.7.5 用户、角色权限关系配置

包括用户角色设置、角色权限关系配置。

2.2.4 系统对接和数据采集需求

本项目中标方需完成相关系统的对接和数据采集工作，调研制定工作计划，编制符合国家标准（如电子病历、互联互通等标准）和我省相关标准的统一接口文档，以保障项目的有效实施与开展，对接内容如下所述。

（1）完成与合肥、池州、宿州三个试点地市共计 18 个试点县区的 3832 家基层医疗卫

生机构系统对接（因基层机构动态调整，具体机构数以项目实施为准），以获取患者健康档案、电子病历、检查检验等信息内容，实现治疗适宜性审核子系统、风险病例审核子系统、专家审核子系统与转诊辅助子系统的功能使用。

（2）可通过市级全民健康信息平台或与医院直接对接等方式，完成与试点区域的 35 家医院对接，实现转诊辅助子系统的功能使用。

3 产品软件需求

3.1 语义理解引擎

用于医疗行业语义相似度度量、业务分类等，为检索引擎、风险识别能力提供支撑。语义理解系统基于深度神经网络的认知和计算能力实现，通过对用户表述的内容进行语义理解和关键信息提取，来帮助相关产品实现用户对话和目关键信息获取的功能；系统功能包括关键信息提取，意图理解，知识库能力，命名体识别等。

（1）关键信息提取

应用场景分为用户意图理解和关键信息提取两大类，在语义解决方案中，对用户的回答文本，首先根据场景区分来进行关键信息的提取。

（2）意图理解

面对文本匹配的需求，最基本的就是评估文本间的相似度；提出的方案是基于 LSTM 来对句子进行建模，通过计算向量相似度来评估不同句式之间的语义相似度。在语义理解引擎的意图应用场景中，采用简化版本的“规则+模型”相结合的解决方案，简便快捷的支持意图理解。应具有很好的可维护性和定制化。

（3）知识库能力

针对线上复杂语义场景，关键信息提取和语义理解可解决绝大多数问题的同时，存在部分难以覆盖的语义场景，系统应为此提供知识库功能，在语义流程中需加入知识库规则解决效果问题以及个性化需求。

（4）命名体识别

在较多场景下，出现药品名，症状，体征等专业名词，需通过统计模型方案来实现命名体识别能力来解决命名实体提取的问题，用于对用户表述中的命名实体进行语义的提取。

3.2 语音识别引擎

语音识别引擎应采用行业先进的语音识别技术，除中文普通话和英文外，还支持多语种识别，可用于不同的医疗场景，如口述书写电子病历、口述医疗文书等。

通过集中部署，以云服务的方式为应用终端提供语音相关服务，通过集成标准的 SDK 控件，为最终用户提供语音识别人工智能应用。对医学领域应用进行深度定制优化，应具有医学文本高识别准确率、医用集成接口更易用等特点。

接入层是面向终端用户的层级，支持接入语音识别能力。

能力层包含引擎能力端和其对应的业务层独立服务，主要为识别能力，通过 nginx 连接所有的独立服务，提供统一的 IP 及端口供 SDK 连接使用。

服务层提供基于平台能力封装的知识问答服务、文本/音频检索服务、数据分析服务、授权服务等核心服务开放，提供基于 RestFul 的服务接口，为第三方业务应用提供有效的服务层支撑。

3.3 医学挖掘引擎

用于挖掘医疗领域文本数据中的医学要素，如症状、体征、疾病、诱因等标签。医学挖掘引擎基于电子病历和医学知识库结合统计模型的深度学习技术获取病历医学专业关键

信息知识点，获取病历中可解释医学知识；然后再利用深度学习模型，基于 bert 的双仿射方案，实现关系提取，最终目的是对病历进行结构化。

（1）Token 提取

应采用模型融合规则的方案，提供将用户输入病历文本中的关键信息进行提取的功能，包括支持症状，诱因，原发病史，呼吸，脉搏等信息提取。

（2）关系提取

对于信息提取来说，单纯获取病历中各类关键信息只是结构化的第一步，而不同类信息间的关系也蕴含着更加丰富的病情信息，应能够进一步提升辅助诊疗效果。

3.4 医学分词能力组件

用于对医疗领域文本数据进行分词结构化，为医学数据结构化能力提供支撑。医学分词能力组件应基于电子病历结合统计模型 crf，对医疗领域病历文本数据进行分词结构化，可为医学数据结构化能力提供支持。

（1）NER 命名实体模块

该模块的主要功能是进行输入文本的命名实体识别，从一段输入中识别出命名实体，应至少包括检查手段、药物药品、手术、症状描述、疾病、检查项、器官组织等。

（2）CWS 中文分词模块

主要是对输入的一段文本进行分词。首先基于 trie 树进行词匹配；其次基于文法规则匹配；然后基于 crf 模型进行序列预测，得到分词结果；最后可将上述结果进行融合，得到最终结果。

3.5 疾病术语标准化能力组件

基于深度学习的模型，对线上医生诊断名称自动进行标准化映射，如映射到 ICD10 编码，用于医学知识图谱建设。

（1）基础字典管理

支持目录管理，包括序号、编码、疾病名称、来源、分类等，疾病多条可分页展示。

（2）基础字典对应

支持导入数据、自动对应、对应状态查看、基础字典对应新增。

3.6 医学同义词推荐引擎

用于医学词典的同义词推荐，如疾病名称、症状标准词、药品名称等，用于医学知识图谱建设。

（1）疾病同义词推荐

对于给定机构，需可以输入疾病同义词或相近词，搜索获得标准词推荐内容。

（2）症状同义词推荐

需可自由输入症状同义词或相近词，搜索获得标准词推荐内容。

（2）药品同义词推荐

对于给定机构，需可以输入药品同义词或相近词，搜索获得标准词推荐内容。

3.7 OCR 识别能力引擎

主要解决的问题是如何将各种医疗场景的图像转换成文字，涉及数字信号处理，计算机科学等多种学科技术。应支持电子病历印刷体、纸质病历手写体识别，支持输出文本行，字符精确位置；支持中，英等多个语种识别；参数：用户可以配置识别的语种（在系统支持的语种范围内），针对中英文，支持速度高低配模式等。

基于深度神经网络实现，通过图像预处理、版面分析、图像要素分块、字符识别等过程对图像中的各种信息进行提取和识别；系统功能包括图像朝向与角度检测、文本行检测与

文字识别、非文字图像目标检测、表格检测与恢复。

（1）印刷体识别

应包括常规文档识别、表格类文档识别、插图类文档识别。

（2）手写体识别

对于文档类图片经常出现印刷体与手写体混排的情况，首先通过文本行检测模型进行印刷体与手写体的分类，即检测文本行的同时给出文本行的属性。

（3）表格重建

针对表格识别与重建功能，采用融合多种特征的深度学习表格检测方案，综合使用图像原始特征，以及对图像进行形态学、距离变换等特征进行输入，需具备较好的鲁棒性和泛化性。

3.8 系统运行监测组件

对不同类型日志进行统一管理，通过关键词检索可快速搜索出异常事件的日志，定位问题节点，结合上下文查询能力将异常事件的调用链完整还原，并投递至对象存储享受集中式的数据存储及生命周期管理。

系统运行监测组件提供关于日志搜索、配置、管理、查看链路调用、统计、分析、跟踪和依赖等工作，为管理员提供了良好、易用的控制台，便于日常工作。需包含日志搜索、日志配置、分组管理和项目管理、调用概况、链路分析、异常列表、链路跟踪和服务依赖等功能模块。

（1）日志搜索：根据搜索条件，查询日志详情

（2）分组管理：用于日志分组的创建，编辑和删除

（3）项目管理：用于日志项目的创建，编辑和删除

（4）日志类型：用于日志类型的创建，查看，编辑和删除

（5）调用概况：查看调用总数，调用趋势图以及调用分布情况

（6）链路分析：统计链路响应时间分布、组件平均响应时间、组件分布、调用次数和QPS

（7）异常列表：查看异常项目信息

（8）链路跟踪：跟踪异常项目的原始信息以及详情信息

（9）组件依赖：查看组件所依赖的服务

3.9 图文存储检索组件

部署私有化存储能力，为业务局点应用提供底层能力支持，保证整体数据流转的通畅性，海量、安全、低成本、高可靠的分布式存储组件，性能基于底层硬件提供，灵活适配各种量级的业务需求，便与业务各组件统一集成，提供封装 token 管理逻辑的 SDK,降低接入和运维难度，提高可维护性。

为了便于各业务系统使用统一对象存储能力，应提供相关的 SDK，可以直接对接统一对象存储网关或者原生对象存储服务，支持 JAVA 版本。

需实现鉴权、对象上传、下载、元数据修改等功能，兼容各业务产品定制的接口，封装相应的 token 管理机制，简化业务方的调用逻辑，降低使用成本。

3.10 多模态分布式消息队列引擎

高可靠、高安全、高扩展、易集成的分布式消息队列引擎，需支持多种消息转发、交换、适配、存储，帮助应用解决分布式系统间传递数据、通知消息，构建松耦合系统。

多模态分布式消息队列引擎是分布式系统中重要的组件，主要解决异构数据存储互通，消除数据孤岛的同步平台，为大数据各系统和业务方提供数据集成的高效通道，实现异构数据源互通集成，包括各种关系数据库、大数据组件，实时数据，文件数据及接口数据等。支

持集成过程中的映射、转换、标准化等预处理，同时提供有效监控服务，实时分析任务运行调度的情况。

可支持顺序消息，事务消息，广播消息，延迟消息等各类型消息，支持推和拉多种消费模式，支持集群部署，支持消息映射转换以及可视化管理等。

3.11 数据交换引擎

解决异构数据存储互通，消除数据孤岛的同步平台，为大数据各系统和业务方提供数据集成的高效通道，实现异构数据源互通集成，包括各种关系数据库、大数据组件，实时数据，文件数据及接口数据等。需支持集成过程中的映射、转换、标准化等预处理，同时提供有效监控服务，实时分析任务运行调度的情况。

通过数据交换引擎的集成使得应用间的数据交换组件化、通用化，主要解决数据的分布性和异构性的问题。

（1）需支持绝大多数关系型数据库、主流的非关系型数据库、HDFS 生态大数据组件、主流的 MQ 中间件、HTTP/TCP 网络接口及 Excel 等文件存储。

（2）需支持分隔符分割的文本、JSON、XML、AVRO 等协议格式的可配置化转换，对复杂的转换规则支持使用嵌入式脚本进行转换。

（3）需支持一数据源对多目标数据存储的分发，多数据源对一目标数据存储的合并，支持对数据流进行任务调度。

（4）可在单条数据粒度上对数据流中的数据进行查看和重放。可将处理失败的数据流入单独队列，对这部分数据进行筛查和统一处理。

（5）需提供可视化运维看板进行引擎的监控。看板上为单条数据流定制监控图表和告警，监控其运行状况。

（6）引擎可根据业务压力进行横向扩展。

3.12 分布式定时调度组件

调度中心基于线程池多线程触发调度任务，快任务、慢任务基于线程池隔离调度，提供系统性能和稳定性；任务调度流程全异步化设计实现，如异步调度、异步运行、异步回调等，有效对密集调度进行流量削峰。

（1）需提供 Web 页面对任务进行管理，管理系统支持用户管理、权限控制；

（2）需支持容器部署；

（3）需支持通过通用 HTTP 提供跨平台任务调度；

（4）需支持页面对任务 CRUD 操作；

（5）需支持在页面编写脚本任务、命令行任务、Java 代码任务并执行；

（6）需支持任务级联编排，父任务执行结束后触发子任务执行；

（7）需支持设置任务优先级；

（8）需支持设置指定任务执行节点路由策略，包括轮询、随机、广播、故障转移、忙碌转移等；

（9）需支持 Cron 方式、任务依赖、调度中心 API 接口方式触发任务执行；

（10）调度中心基于线程池多线程触发调度任务，快任务、慢任务基于线程池隔离调度，提供系统性能和稳定性；

（11）任务调度流程全异步化设计实现，如异步调度、异步运行、异步回调等，有效对密集调度进行流量削峰；

（12）任务调度中心、任务执行节点均集群部署，需支持动态扩展、故障转移；

（13）需支持任务配置路由故障转移策略，执行器节点不可用是自动转移到其他节点执行；

（14）需支持任务超时控制、失败重试配置；

（15）需支持任务处理阻塞策略：调度当任务执行节点忙碌时来不及执行任务的处理策略，包括：串行、抛弃、覆盖策略；

（16）需支持设置任务失败邮件告警，预留接口支持短信、钉钉告警；

（17）需支持实时查看任务执行运行数据统计图表、任务进度监控数据、任务完整执行日志。

4 系统集成需求

负责与本项目有关的全部集成工作，及与集成工作相关的一切事务，集成服务主要涵盖从硬件环境准备就绪后开始进行工勘、方案设计、平台部署，验收测试、运维使用等一系列服务内容，帮助采购人建造稳定、可靠的“智联网医院”平台

4.1 集成服务范围

1）完成“智联网医院”平台规划与设计，提供硬件需求清单、硬件设备出厂设置要求、软件测试方案等内容。

2）负责“智联网医院”平台建设的项目管理和实施，产品测试等工作。

3）根据采购人需求，中标方提供“智联网医院”平台建设所需要的信息，包括 IP 地址，域名，服务器地址等信息，以及需要协助的其它信息。

4）完成“智联网医院”平台硬件环境搭建及全网联调、测试、验收等工作。

5）完成“智联网医院”应用系统软件的部署、联调、测试、验收等工作。

4.2 集成服务内容

1）项目管理：对项目进行整体进度、资源、风险把控和控制。

2）现场工勘：现场机房工勘，机柜、布线，输出工勘报告。

3）实施方案规划：根据工勘结果和采购人需求输出规划设计方案。

4）布线方案设计及核查：根据工勘结果输出布线方案，并对布线进行核查，输出布线测试报告。

5）布线施工：完成布线施工。

6）设备安装指导与监控：在采购人现场指导采购人按照标准进行基础设施建设工作，包括追踪硬件及建材采购流程跟踪及到货信息确认，指导施工队进行硬件部署。

7）基础网络搭建：在采购人服务器、网络设备等硬件到货、上架并且数据中心基础设施等按照要求准备完毕之后，根据网络架构方案进行网络设备的调试和部署。

8）操作系统部署：针对服务器的不同用途和服务器类型进行操作系统安装。

9）产品部署：基于采购人采购的产品，进行产品安装调试工作。

10）功能测试：对“智联网医院”平台的功能进行测试，确保平台达到可交付水平。

11）平台验收：按照项目验收流程进行验收，提交交付物。

12）服务支持：包括实施过程中问题解决，方案核对，配置文件核对工作。

5 软件测评需求

针对本项目建设内容中标方选择一家符合资质要求的软件测评机构按照采购人要求客观开展第三方软件测评，并提供相关技术咨询服务，对项目建设的质量把关，确保项目建设实现预期建设目标，符合设计需求，满足工程建设项目审批管理业务的应用和开展。

5.1 软件测评机构资质要求

1、具有计量认证（CMA）证书；

2、具有国家认可委（CNAS）证书。

5.2 测试范围

软件测评机构需提供项目验收测试服务，评估项目的完成情况，客观公正评测项目是否满足招标文件、项目合同以及设计方案的要求，对项目建设中用到的系统软件功能进行必要的检测，把控系统质量关，评测功能相关特性、性能、代码和数据安全性是否达到建设目标，文档是否完备，最终形成项目的验收评测报告，作为项目验收的依据。

测试范围包含但不限于本次项目所有建设内容。

5.3 测试实施要求

1）软件测评机构应按照采购人的要求制定详细的及项目实施计划，在项目实施计划由采购人确定后，进入实施阶段。

2）软件评测对象为项目开发的软件和系统，评测内容包括软件产品的功能、性能效率、兼容性、易用性、可靠性、维护性、可移植性、信息安全性的质量特性，以及用户文档集等文档特性。

3）软件测评机构需针对本项目组建项目团队，指派检测项目经理一名，全权负责本项目的检测活动的组织与管理。评测人员应以公正、科学、客观、准确的态度，严格按照《系统与软件工程 系统与软件质量要求和评价（SQuaRE 第 51 部分：就绪可用软件产品（RUSP）的质量要求和测试细则》（GB/T 25000.51 016）等国家有关标准规定的评测方法，开展项目软件评测工作。

4）评测人员应加强与采购人的沟通。在项目软件评测过程中，须及时向采购人通报在系统中发现的问题，并于系统评测完成时向采购人提供一份详实的评测报告。如评测中发现要修正的问题，待修改完后，要进行一次回归评测。

5.4 测试工作环境

测试工作过程中的测试系统和测试环境由采购人提供，软件测评机构需提供相关测试人员、测试工具、测试设备。

5.5 全过程测试

本次测试是按照开发阶段来进行的，软件测评机构需全程参与该项目的测试工作。

5.6 保密要求

本项目的内容涉及安徽省“智联网医院”试点项目的所有资料都视为采购人拥有的商业秘密，所以软件测评机构有责任和义务保证项目所涉及全部内容的保密和安全，不得在其他任何场合以任何手段使用。对于本项目中所涉及的全部内容的安全保密，软件测评机构应在项目实施前与采购人签订保密协议。对于软件测评机构未经采购人书面同意，以任何方式和渠道泄露秘密的情况，软件测评机构将承担由此造成的一切损失并承担法律责任。

5.7 项目交付物

在项目执行过程中，软件测评机构需按约定，及时、完整、准确地交付合格的交付文档。

1）评测计划：应包含测试的进度安排、人力资源计划、质量保证、风险管理、沟通管理等内容。

2）评测方案：应包含系统评测全部相关内容。

3）执行记录：完成评测方案中的所有测试内容，并填写详细测试记录。

4）评测脚本：性能测试脚本应覆盖所有性能测试内容。

5）问题报告：提交完整的问题报告，应包括问题描述、状态、严重程度、优先级等内容。

6）评测报告：提交正式评测报告，报告中应充分覆盖软件测试相关内容。

6 项目管理要求

为保证项目按计划进度顺利推进，中标方需对项目管理组织体系、质量管理与控制、风险分析与管理、项目运维管理、项目培训计划等方案进行详细描述。

中标方制定项目实施管理方案，提供足够数量的项目开发实施专业技术团队，其中开发团队不得少于 20 人（包括 1 名项目负责人），实施团队驻点专业技术人员不少于 10 名（包括 1 名项目负责人），保证系统开发、调试、安装、培训等各项工作顺利进行。项目实施前提供以上资料供采购人核实。

7 项目实施进度要求

本项目实施周期为：自签订合同之日起 180 个日历天建设完成。

中标方需要提供完善、合理的实施进度计划，并通过完善的项目实施保障措施，保证本项目顺利上线。

8 人员培训要求

以本项目部署的所有医疗卫生单位能够掌握“智联网医院”系统各项功能的应用为前提，中标方提供相应的应用软件技术和系统操作等方面的培训，提供培训教材，培训应该在本期项目验收完成前进行。培训方式：按省级、市级、县（区）级对全部用户开展免费现场培训。

中标方应在响应文件中提出全面、详细的培训计划，并在合同签订后征得采购人同意后实施。中标方应提供面向系统管理员的维护、配置、以及安装等方面的培训。

9 售后服务要求

中标方应具备本地化服务能力，能提供快速的售后服务响应，售后服务驻点人员不低于 6 人（包括 1 名项目负责人）。项目负责人变更前需提前 15 个日历日征求中心意见。项目实施前提供以上资料供采购人核实。

（1）中标方应有良好的服务理念和完善的售后服务体系，能够提供本地技术服务。

（2）针对本项目，提出完整而切实可行的服务方案。其中，至少应提供 7×24 小时热线电话、远程网络等服务方式。热线电话和远程网络提供技术咨询和即时服务，1 小时内给予明确的响应并解决；现场服务适用于排解重大故障。

（3）质保期：从项目验收通过之日起 3 年，第一年包括中标方须无条件满足招标方全部的升级改造需求，后两年为常规性维护。质量保证期内，服务内容包括:协助采购人完成日常系统及应用的维护工作，保证系统的稳定正常运行；问题、故障的诊断与排除，系统配

置和辅助应用系统部署与维护；软件版本的升级、调试。

（4）质保期过后，维护费不高于合同价的 8%，具体由采购人和中标方通过维保合同或协议商定。

中标方在投标方案中应提供详细的售后服务内容、措施、响应时间等内容。

10 采购清单

10.1 软件开发需求清单

序号	品目名称	技术指标	单位	数量
1	核心能力平台	核心能力平台为位于系统的能力层，通过对核心服务的封装为上层业务提供能力支撑。根据本项目业务需要，核心能力平台包括医学数据结构化能力、基于知识图谱的知识推理能力、基于深度学习的医学语义度量能力、基于深层次语义理解的医学检索知识服务、面向用户的结构化知识问答展示服务、面向业务应用的推理知识共享服务、高风险诊断识别检测能力、高风险症状识别监测能力、治疗适宜性识别监测能力、诊疗效果监测评估能力等。	套	1
2	信息支撑平台	信息支撑平台是整体智联网医院系统建设的重要技术平台支撑，用以提供给上层子系统集成调用。主要包括数据访问权限控制模块、数据脱敏模块、数据加密模块、结构化数据交换模块、医疗信息模型化转换模块、医疗数据文档化存储模块、医疗对象索引标识化模块、基于消息队列的数据处理模块、消息提醒服务等。	套	1
3	治疗适宜性审核子系统	治疗适宜性审核子系统通过调用治疗适宜性审核能力模型，基于医学认知智能技术和医学知识体系，针对治疗的适宜性进行分析并能开展常见治疗风险问题的监测。主要包括基于相似认知的数据映时管理模块、治疗适宜性规则管理模块、治疗适宜性监测告警模块、基于病情数据的专家咨询、记录管理中心等。	套	1
4	风险诊疗病例评估子系统	系统通过对接“智医助理”系统，获取到基层医生在当前诊疗过程中产生的业务数据，通过将当前诊疗数据和系统收集到的既往信息数据与核心能力平台进行交互，获取到核心能力平台反馈的风险判断结果，如出现风险项，则在诊疗过程中需要及时给与医生提醒，便于医生进行及时关注与修改。主要包括面向多系统业务调用的支持模块、风险诊疗病例评分模块、基于 RW 值测算的病情综合评估、风险内	套	1

		容等级评估特异性配置、风险等级证据可视化指示等。		
5	专家审核子系统	当系统发现风险病例后或有基层医生提出问题后，相应的数据均会进入“专家审核子系统”。由不同层级的上级医生进行审核与指导。首先，在县域医共体下，基层医生遇到相应问题，首先提交至县级医院医生层面，如能解决问题，则会形成审核结论以及提醒下达给基层医生，并对基层医生开展疑问解答。主要包括多模态融合交互引擎、统一任务服务、基于BS 架构的专家审核网页端、基于安卓架构的专家审核移动端等。	套	1
6	转诊辅助子系统	系统通过对接“智医助理”系统，获取到基层医生在当前诊疗过程中产生的业务数据，当基层机构遇到实施救治的病例或受诊疗条件限制不能诊治的疑难复杂病历、疾病诊治超出本机构核准诊疗科目的病例时，可进行患者的转诊。系统通过对接能帮助转出医生更少的进行信息录入，接收的医生更多的查阅信息内容。主要包括转诊资源与关系配置管理、转诊条件管理、机构与资源质量评估、适宜资源智能推荐、转诊发起端、转诊审批端、转诊接收端等。	套	1
7	患者应用子系统	支持支持患者通过系统调用自己的电子健康卡，进行身份验证、服务登记等各项业务内容的开展。居民还能通过该系统对当前的诊疗服务进度进行跟踪，完成服务后对服务质量进行评价。同时为便于系统推广与使用，与省内“皖事通”等相关系统进行对接与挂载，进一步便于广大居民使用。主要包括患者信息自助模块、电子健康卡调用、服务进度跟踪管理、服务评价模块	套	。1
8	监管统计子系统	建设监管统计子系统，系统需要进行数据元管理，并通过数据治理、数据集成、监管业务建模，实现各类业务开展情况的可视化监管呈现，并提供项目运行管理驾驶舱等功能模块。	套	1
9	基础管理子系统	基础管理子系统需要面向参与“智联网医院”的机构与部门管理人员使用，支持“智联网医院”注册与登录机构管理、人员账号管理、功能与数据权限调整，保障“智联网医院”后台的有效运营和维护，支撑前端人员更好的使用。	套	1
10	系统对接和数据采集	完成相关系统的对接和数据采集工作，调研制定工作计划，编制符合国家和省里标准（如电子病历、互联互通等标准）的统一接口文档，	项	1

		以保障项目的有效实施与开展。		

10.2 产品软件需求清单

序号	品目名称	技术指标	单位	数量
1	语义理解引擎	用于医疗行业语义相似度度量、业务分类等，为检索引擎、风险识别能力提供支撑。	套	1
2	语音识别引擎	行业先进的语音识别技术，除中文普通话和英文外，支持多语种识别，可用于不同的医疗场景，如口述书写电子病历、口述医疗文书等。	套	1
3	医学挖掘引擎	用于挖掘医疗领域文本数据中的医学要素，如症状、体征、疾病、诱因等标签。	套	1
4	医学分词能力组件	用于对医疗领域文本数据进行分词结构化，为医学数据结构化能力提供支撑。	套	1
5	疾病术语标准化能力组件	基于深度学习的模型，对线上医生诊断名称自动进行标准化映射，如映射到 ICD10 编码，用于医学知识图谱建设。	套	1
6	医学同义词推荐引擎	用于医学词典的同义词推荐，如疾病名称、症状标准词、药品名称等，用于医学知识图谱建设。	套	1
7	系统运行监测组件	对不同类型日志进行统一管理，通过关键词检索可快速搜索出异常事件的日志，定位问题节点，结合上下文查询能力将异常事件的调用链完整还原，并投递至对象存储享受集中式的数据存储及生命周期管理。	套	1
8	图文存储检索组件	部署私有化存储能力，为业务局点应用提供底层能力支持，保证整体数据流转的通畅性，海量、安全、低成本、高可靠的分布式存储组件，性能基于底层硬件提供，灵活适配各种量级的业务需求，便与业务各组件统一集成，提供封装 token 管理逻辑的 SDK,降低接入和运维难度，提高可维护性。	套	1
9	OCR 识别能力引擎	主要解决的问题是如何将各种医疗场景的图像转换成文字，涉及数字信号处理，计算机科学等多种学科技术，支持电子病历印刷体、纸质病历手写体识别，支持输出文本行，字符精确位置；支持中，英等多个语种识别；参数：用户可以配置识别的语种（在系统支持的语种范围内），针对中英文，支持速度高低配模式等。	套	1
10	多模态分布式消息队列引擎	一种高可靠、高安全、高扩展、易集成的分布式消息队列引擎，支持多种消息转发、交换、适配、存储，帮助应用解决分布式系统间传递数据、通知消息，构建松耦合系统。	套	1

11	数据交换引擎	解决异构数据存储互通，消除数据孤岛的同步平台，为大数据各系统和业务方提供数据集成的高效通道，实现异构数据源互通集成，包括各种关系数据库、大数据组件，实时数据，文件数据及接口数据等。支持集成过程中的映射、转换、标准化等预处理，同时提供有效监控服务，实时分析任务运行调度的情况。	套	1
12	分布式定时调度组件	调度中心基于线程池多线程触发调度任务，快任务、慢任务基于线程池隔离调度，提供系统性能和稳定性；任务调度流程全异步化设计实现，如异步调度、异步运行、异步回调等，有效对密集调度进行流量削峰。	套	1

10.3 系统集成需求清单

序号	品目名称	技术指标	单位	数量
1	系统集成	负责与本项目有关的全部集成工作，及与集成工作相关的一切事务。	项	1

10.4 软件测评需求清单

序号	品目名称	技术指标	单位	数量
1	软件测评	通过第三方软件测评，测评项至少包含软件功能、性能、安全、文档等内容	项	1

11 其他要求

11.1 中标方所提供的软件产品、数据库、中间件等相关内容不得引起与采购人有关的任何法律纠纷，若引起由中标人承担一切责任，并提供承诺函；

11.2 本项目所开发软件的版权归采购人所有，中标方须提供源代码、开发文档。采购人可以授权中标方二次开发后出售。提供承诺函。

11.3 中标方承诺配合完成等保测评相关工作。

11.4 中标方及其开发、实施、售后服务人员均要和采购人签订保密协议。

11.5 项目绩效和使用效果评价

项目绩效和使用效果评价作为本项目验收资料之一，主要以用户满意度、服务量等为依据，具体内容如下：

（1）关键用户（基层医生及患者）：对系统的总体评价、未满足之需求的接受程度。

居民与患者对基层医疗卫生机构的服务能力评价，是否由于“智联网医院”体系解决了寻求医疗资源的需求。

（2）决策层（卫生健康委相关部门）：决策层对系统的总体评价、不满意之处。

（3）解决问题的程度：与项目最初预定要解决之问题的差距是否在可接受范围内、需立即解决还是后续解决。

（4）项目进度类：覆盖县区数、接入单位数、总体用户数等；

02 包采购需求

1、配置参数要求

序号	品目名称	技术指标	单位	数量
1	存储资源扩容	1.现有 HPE、3PAR StoreServ 8440 存储扩容，能够与现有双活系统无缝对接，实现平滑升级扩容； ★2.扩容现有“智医助理”双活存储系统，每台配置≥2 个 24 盘位硬盘扩展柜，≥48 块 1.8T 10K SAS 硬盘，扩容后的资源加入双活系统。 ★3.支持硬盘扩展柜掉电或故障时保持业务不中断，数据不丢失，提供扩展柜级的数据保护机制； 4.扩容的硬盘与现有硬盘利用底层虚拟化技术，在硬盘故障的情况下能够多对多高速重建，同一块硬盘上可以同时存在 RAID0/1/5/6/10/50/60 等不同的 RAID 类型； ★5. 为保证项目顺利的实施，保证现有平台的稳定和数据的安全，本项目需提供原厂工程师实施，并提供原厂商出具的服务承诺；	套	2
2	虚拟化软件扩容	1.现有 H3C 虚拟化平台 VC-CAS-ENT 扩容 32 颗物理 CPU 虚拟化软件授权，含部署服务； ★2、提供将现有部分虚机迁移至本平台的服务，并提供详细迁移方案； ★3. 为保证项目顺利的实施，保证现有平台的稳定和数据的安全，本项目需提供原厂工程师实施，并提供原厂商出具的服务承诺；	套	1
3	▲虚拟化宿主机	1.品牌规格：国产品牌、非 OEM，2U 机架式服务器； ★2.处理器：配置 2 颗 CPU，主频≥2.3G，核心数≥18，L3 缓存≥24MB； ★3.内存：配置 256GB ECC DDR4 2666MHz（32GB*8），支持 24 根内存插槽； ★4.硬盘：配置 4*480GB SSD 硬盘， 最大支	台	8

		持 40 块硬盘； 5.RAID:配置独立 Raid 卡（2GB 缓存，含电池保护），Raid 1/0/10/5/50/6/60 级别； 6.网卡：2 个万兆 2 端口 SFP+网卡，4 个高性能千兆网口； 7.HBA 卡：配置 2 块双口 16G HBA 卡（含 4 个 16G 模块）； 8.带独立带外管理口； 9.配件：配置机架安装导轨； 10.电源：配置 1+1 冗余电源； 11.管理功能：集成系统管理芯片，支持 IPMI2.0、KVM over IP 等管理功能，配置原厂中文服务器管理软件。		

2、供货及安装期限要求

合同签订后 15 个工作日内供货、安装、调试完毕。

3、供货及安装地点要求

安徽省合肥市，采购人指定地点。

4、免费质保期要求

验收合格之日起原厂免费质保三年，中标后提供原厂售后服务承诺函。

5、报价要求

本项目报总价，采购人后期不予增加任何费用，投标人须自行考虑投标风险。

6、其他要求

1、中标方全部集成工作要保证与原有平台或系统无缝对接。提供承诺函。
2、中标方及其实施人员均要和采购人签订保密协议。提供承诺函。

03 包采购需求

服务要求

1 项目概况

针对安徽省“智联网医院”试点项目提供监理服务。

2 服务范围

总体实施方案和设计方案的质量把关，工程进度控制，投资控制，信息管理，建设安全管理，系统测试，系统集成调试，项目培训，系统试运行和验收工作的监理，系统移交及相关文档的起草和管理等工作，确保项目质量、进度和投资计划的顺利实施，做好项目合同与文档（资料）管理，受采购人委托，负责协调项目涉及的各承建单位之间的工作关系，并协调解决项目建设过程中的各类纠纷，针对项目建设情况，向采购人提出合理化的改进改良建议，并提供监理服务。

3 服务要求

确保项目实施方按照设计方案，招标、投标文件及合同要求实施项目建设，对承建方进行有效的监督和配合，确保工程保质、按时完成。

制定针对本次项目建设的监理工作计划；对到货设备逐一进行检查核对，跟踪软件系统的开发过程；对照项目建设方案，督促承建方提交详细施工方案和进度计划，协助业主单位审核施工方案和进度计划，并监督工程建设方遵照实施；配合采购人对项目进行功能、性能测试，配合采购人验收；对工程安全、信息和知识产权等实施规范的管理（确保采购人数据信息不外泄等）。

4 服务质量标准

项目实施应使用与本项目内容相关的下列最新版本的标准与规范：

1.服务合同；

2.项目招标文件；

3.采购人与承建单位签订的施工合同；

4.合同图纸及说明；

5.国家、项目所在地颁布的法律、法规等；

6.采购人授予的其他权限。

5 服务内容

监理方要对项目实施时的关键点进行监理，而且要全方位地开展监理工作。按照相关国家标准，监理工作内容包括但不仅限：质量控制、进度控制、投资控制、合同管理、信息管理和组织协调等，包括但不限于以下内容：

5.1 质量控制

依据有关的项目文件、合同和设计单位制定的技术规范书，审查、监督、控制各子项目的质量。通过事前预防、事中控制、事后纠正等措施，依据国家法律、法规、标准以及项目合同、设计方案、监理规划、监理实施细则等文件控制工程质量。

事前质量控制

1)了解采购人的业务需求，并将其作为监理工作的依据。

2)对验收方法、接收准则、时间进度的要求提出监理意见。

3)协助合同编制，对合同提出监理意见。

事中质量控制

1)审核承建方提交的工程设计方案：

与项目合同、需求的符合性；

关键技术的实现方法、流程及技术保障措施的合理性；

实施的质量保证措施的可行性;

实施组织机构保证。

2)对承建方提供的软硬件货物进行验收，对验收结果做验收记录，并经三方签认；对不符合合同或相关标准规定的货物拒绝签认。确保没有被签认的货物不得在工程实施中应用。

3)检查承建方项目实施状况、人员与实施方案的一致性；

4)阶段性质量监督、控制措施及方法，并做监理日志。出现工程质量问题时，经确认后监理机构签发监理通知单，报业主、承建方，责令承建方整改。

5)及时处理承建方提交的工程中关键环节的实施申请，审核其合理性后签认，报采购人批准。

6)检查承建方重要工程步骤的衔接工作，做监理日志。

7)及时处理变更申请，审核变更的合理性，保证工程总体质量、进度不受影响。

8)按照监理细则规定的程序处理工程中出现的质量事故。组织软件工程质量、系统集成质量事故的原因调查、问题分析、问题评估、事故处理；

9)若发现实施过程存在重大质量隐患，应及时向承建方签发停工令，并报采购人，监督承建方进行整改。整改完毕后，及时处理承建方的复工申请。

事后质量控制

1)按照国家信息化项目管理流程，协助采购人和承建方完成项目初验和终验。

2)协助采购人审核承建方提交的验收计划及其方案，明确验收目标、各方责任、验收内容、验收标准、验收方式和验收结果等内容，审核后签署监理审核意见。

3)协助采购人对初验中发现的质量问题进行评估，根据质量问题的性质和影响范围，确定整改要求和整改后的验收方式，以监理通知单的形式告知承建方。

4)监督承建方根据整改要求提出整改方案，并监督整改过程。

5)对软件项目开展功能及性能测试工作，提交测试报告；对硬件项目开展检验检测，提交检测报告。

6)与采购人和承建方共同确认初验结果，签署初验合格报告。

7)监督系统的试运行，督促承建方解决试运行中出现的质量问题。

8)确认项目达到终验条件，协助采购人组织工程终验。

9)督促承建方完成项目实施方案中确定的培训，并对培训效果做出评估。

10)跟踪各子项目在质保期内的运行状况，督促承建方做好售后服务。

5.2 进度控制

审查项目进度计划，并监督计划的执行，通过事前预防、事中控制、事后纠正的措施，

确定工作顺序，控制项目进度。

事前进度控制

1)协助编制项目工作计划，分析工程的内容及过程，对工程进度提出监理意见。

2)对工程合同中涉及的产品和服务的提供时间做出说明，并对采购人的安排提出监理意见。

事中进度控制

1)审核承建方提交的工程进度计划的可行性、合理性、各阶段工作成果，签署监理审核意见。

2)根据工程进度计划，确定阶段性进度监督、控制的措施及方法，作为监理细则的内容。

3)审核承建方开工申请，检查工程准备情况，签发开工令，并报采购人签认，通知承建方开始工程实施。

4)督促承建方提交阶段性进度计划，审核阶段性进度计划合理性，签署审核意见。

5)定期检查、记录工程的实际进度情况，确保实际进度与计划相一致；

6)发现工程未能按计划进行时，要求承建方调整或修改计划，采取必要措施加快开发进度，以使实际项目进度符合合同的要求。

7)当项目进度可能导致合同工期严重延误时，详细报告分析原因和提出对策，供采购人采取措施或做出决定。

事后进度控制

对验收阶段进度安排提出监理意见。

5.3 投资控制

1)动态管理跟踪项目建设成本，进行成本、费用控制和分析；

2)审查系统建设进度款申报；

3)严格控制和审查工程变更，核算成本和变化量，报业主审批；

4)审核施工方的工程量清单和工程竣工结算。

5.4 合同管理

协助采购人与承建方签订合同；监督承建方履行合同；协助采购人处理合同执行过程中的违约、索赔、延期、纠纷调解及仲裁等问题。

5.5 信息管理

及时向采购人反映项目实施的动态信息，提交监理工作情况的工作文档。

建立全面、准确反映实施阶段状况的图表、文档，收集和管理项目各类文档资料。

完成实施过程中各类工程日志、会议纪要、备忘录、电子邮件、传真、电话记录等资料，完成资料的整理、审核和归档工作；

督促承建方及时完成各阶段设计文档、程序代码、测试记录、变更记录、问题跟踪处理记录等文件的归档工作，按归档要求进行分类整理归档，按时完成竣工验收资料（包括监理工作方面的资料），确保软件工程中各类文件传送的规范化、制度化。

监理方的文档管理人员负责收集、管理监理工作各类文书资料，对监理工作文档、收发文签收登记等进行管理。

5.6 组织协调

1)协助采购人划分各方的工作范围和职责。

2)监督项目各方履行职责，协调各方的工作关系。

3)建立畅通的沟通渠道，采取有效措施使项目信息在有关各方之间保持顺畅流通，积

极协调项目各方之间的关系，推动项目实施过程中问题的有效解决。

5.7 变更控制

1)对项目变更控制，明确界定项目变更的目标，防止变更范围的扩大化，加强变更风险以及变更效果的评估。

2)对变更申请及时响应；任何变更都应在实施前进行评估，选择冲击最小的变更方案。

3)任何变更都要得到采购人单位、监理单位和承建单位三方共同签字的书面确认。

5.8 项目安全管理

1)确立项目建设安全监管制度体系和工作目标。

2)审核项目建设安全保密工程技术方案。

3)排查与处理项目建设安全隐患。

6 人员配备

岗位	人员资格及要求	数量
总监理工程师	具有信息系统监理师证和信息系统项目管理师证书，具备5 年及以上信息系统监理经验，不允许外聘、返聘、更换	1 人
专业监理工程师	具有信息系统监理师证书证书，具有 2 年及以上信息系统监理经验，不允许外聘、返聘、更换	2 人
监理员	不允许外聘、返聘	2 人
合计：5 人		

7 其他

1、中标方的技术方案中应含有监理大纲和监理方案，其中监理方案要求包括从项目需求到系统验收全过程，包括建设内容、监理要求、监理内容、质量管理方式、组织实施、进度安排、培训与售后服务、系统分阶段验收和最终验收等。监理方案应明确监理的各项运行过程，包括监理人员的相关资料、职能分配及工作流程，各项监理工作的相关负责人等，并认真履行全过程监理职责；

在本合同期内及合同终止后，未征得采购人同意，不得泄露与本项目有关的资料；

如承建单位在项目实施中不符合项目规范和质量要求，监理方要监督承建单位停工整改或返工；

如果承建单位违反合同规定的质量要求和完工时限，监理方应协助建设单位追究有关承建单位的责任；

监理方使用建设单位提供的设备和物品属建设单位所有，在监理工作完成或终止时，应将设备和剩余物品在合同规定的时间和方式移交给建设单位。

2、专业监理工程师必须长期驻点建设单位，因事离岗需经采购人同意。原则上不得擅自离岗，否则采购人将上报相关管理部门对监理方进行处罚。

监理方及其监理人员均要和采购人签订保密协议。

04 包采购需求

一、项目概况

2019 年 5 月国家标准化管理委员会发布了新修订的《信息安全技术-网络安全等级保护

基本要求》（GB/T 22239-2019）,为贯彻落实国家信息安全等级保护制度，满足国家和安徽省相关考核要求，进一步加强安徽省卫生健康委员会信息中心安全防护能力。为深入贯彻落实习近平总书记关于网络安全工作的重要指示精神和《网络安全法》，进一步推动落实中华人民共和国卫生部《卫生行业信息安全等级保护工作的指导意见》（卫办发[2011]85 号）文件中关于在卫生健康行业全面开展信息安全等级保护定级备案、建设整改和等级测评等工作的要求。根据公安部、国信办联合印发《信息系统安全等级保护管理办法》（公通字[2007]43号）、《关于信息系统安全等级保护工作的实施意见》（公通字[2004]66 号）、《关于开展全国重要信息系统安全等级保护定级工作的通知》（公信安[2007]861 号）等相关文件要求，组织开展信息系统等级保护测评工作，通过项目实施，查找漏洞，整改隐患，切实提高其信息安全防护能力，为全面提高信息系统稳定运行提供安全保障。

二、服务需求

(一) 系统网络安全等级保护测评

依据国家相关文件、标准、系统安全保护等级和 GB/T 22239-2019《信息系统安全等级保护测评要求》，按年对下表中的重要信息系统进行等级保护测评。

序号	系统名称	系统等级
1	“智联网医院”系统	第三级

被测系统描述：

“智联网医院”向下对接安徽省基层医疗卫生机构，向上对接各地市试点医院，并通过“智联网医院”平台构建的人工智能基础能力、标准化医学知识共享能力、诊疗风险自动检测评估能力，促进诊疗资源精准对接、高效医疗服务、政府科学决策，推进区域构建高效医疗卫生服务体系，助力安徽省在全国率先构建面向基层的人机协同诊疗模式

（二）技术要求

1.测评依据标准及参考文件

《信息安全等级保护管理办法》（公通字[2007]43 号）

《信息安全技术信息系统安全等级保护基本要求》GB/T 22239-2019

《信息安全技术信息系统安全等级保护定级指南》GB/T 22240-2020

《信息安全技术信息系统安全等级保护实施指南》GB/T 25058-2010

《信息安全技术信息系统安全等级保护测评要求》GB/T 28448-2019

《信息安全技术网络安全等级保护安全设计技术要求》（GB/T25070-2019）

《信息安全技术信息系统安全等级保护测评过程指南》GB/T 28449-2018

《信息安全技术信息系统安全管理要求》GB/T 20269-2006

《互联网安全保护技术措施规定》（公安部令第 82 号）

《安徽省卫生行业信息安全等级保护工作实施指南》（试行）

2.测评实施原则

（1）保密原则：对测评的过程数据和结果数据严格保密，未经授权不得泄露给任何单位和个人,不得利用此数据进行任何侵害采购人的行为,否则采购人有权追究供应商的责任。

（2）标准性原则：测评方案的设计与实施应依据国家等级保护的相关标准进行。

（3）规范性原则：供应商工作中的过程和文档，具有很好的规范性，可以便于项目的跟踪和控制。

（4）可控性原则：测评服务的进度要跟上进度表的安排，保证采购人对于测评工作的可控性。

（5）整体性原则：测评的范围和内容应当整体全面，包括国家等级保护相关要求涉及的各个层面。

（6）最小影响原则：测评工作应尽可能小的影响系统和网络，并在可控范围内；测评工作不能对现有信息系统的正常运行、业务的正常开展产生任何影响。

供应商应严格依照上述原则和国家等级保护相关标准开展项目实施工作。

3.技术方案要求

工作内容：依据国家等级保护相关标准《GB/T 22239-2019 信息安全等级保护基本要求》和《GB/T 22240-2020 信息安全等级保护定级指南》为基础，进行三级等级保护测评，内容包括：

安全技术测评：包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心五个方面的安全测评。

安全管理测评：包括安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理五个方面的安全测评。各版块测评控制点和要求项如下：

（1）安全物理环境

安全控制点	安全要求项
物理位置选择	要求点a）机房场地应选择在具有防震、防风和防雨等能力的建筑内；
	要求点b）机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。
物理访问控制	要求点a）机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。
防盗窃和防破坏	要求点a）应将设备或主要部件进行固定，并设置明显的不易除去的标识；
	要求点b）应将通信线缆铺设在隐蔽安全处；
	要求点c）应设置机房防盗报警系统或设置有专人值守的视频监控系统。
防雷击	要求点a）应将各类机柜、设施和设备等通过接地系统安全接地；
	要求点b）应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。
防火	要求点a）机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；
	要求点b）机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；
	要求点c）应对机房划分区域进行管理，区域和区域之间设置隔离防火措施。
防水和防潮	要求点a）应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；
	要求点b）应采取措施防止机房内水蒸气结露和地下积水的转移与渗透；
	要求点c）应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。
防静电	要求点a）应采用防静电地板或地面并采用必要的接地防静电措施；
	要求点b）应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。
温湿度控制	要求点a）应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。
电力供应	要求点a）应在机房供电线路上配置稳压器和过电压防护设备；
	要求点b）应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求；
	要求点c）应设置冗余或并行的电力电缆线路为计算机系统供电。
电磁防护	要求点a）电源线和通信线缆应隔离铺设，避免互相干扰；

安 全 控 制 点	安 全 要 求 项
	要求点 b）应对关键设备实施电磁屏蔽。

（2）安全通信网络

安 全 控 制 点	安 全 要 求 项
网络架构	要求点 a）应保证网络设备的业务处理能力满足业务高峰期需要；
	要求点 b）应保证网络各个部分的带宽满足业务高峰期需要；
	要求点 c）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；
	要求点 d）应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段；
	要求点 e）应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。
通信传输	要求点 a）应采用校验技术或密码技术保证通信过程中数据的完整性。
	要求点 b）应采用密码技术保证通信过程中数据的保密性。
可信验证	要求点 a）可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

（3）安全区域边界

安 全 控 制 点	安 全 要 求 项
边界防护	要求点 a）应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信；
	要求点 b）应能够对非授权设备私自联到内部网络的行为进行检查或限制；
	要求点 c）应能够对内部用户非授权联到外部网络的行为进行检查或限制；
	要求点 d）应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。
访问控制	要求点 a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；

安全控制点	安全要求项
	要求点 b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；
	要求点 c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；
	要求点 d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力；
	要求点 e）应对进出网络的数据流实现基于应用协议和应用内容的访问控制。
入侵防范	要求点 a）应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为。
	要求点 b）应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为；
	要求点 c）应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析；
	要求点 d）当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。
恶意代码和垃圾邮件防范	要求点 a）应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。
	要求点 b）应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。
安全审计	要求点 a）应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
	要求点 b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
	要求点 c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；
	要求点 d）应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。

安全控制点	安全要求项
可信验证	要求点a）可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

（4）安全计算环境

安全控制点	安全要求项
身份鉴别	要求点a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性， 身份鉴别信息具有复杂度要求并定期更换；
	要求点b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；
	要求点c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；
	要求点d）应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。
访问控制	要求点a）应对登录的用户分配账户和权限；
	要求点b）应重命名或删除默认账户，修改默认账户的默认口令；
	要求点c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；
	要求点d）应授予管理用户所需的最小权限，实现管理用户的权限分离；
	要求点e）应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；
	要求点f）访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；
	要求点g）应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。
安全审计	要求点a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
	要求点b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
	要求点c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；
	要求点d）应对审计进程进行保护，防止未经授权的中断。
入侵防范	要求点a）应遵循最小安装的原则，仅安装需要的组件和应用程序；
	要求点b）应关闭不需要的系统服务、默认共享和高危端口；
	要求点c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；

安全控制点	安全要求项
	要求点 d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；
	要求点 e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞；
	要求点 f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。
恶意代码防范	要求点 a）应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。
可信验证	要求点 a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证， 在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
数据完整性	要求点 a）应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；
	要求点 b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。
数据保密性	要求点 a）应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；
	要求点 b）应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。
数据备份恢复	要求点 a）应提供重要数据的本地数据备份与恢复功能；
	要求点 b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；
	要求点 c）应提供重要数据处理系统的热冗余，保证系统的高可用性。
剩余信息保护	要求点 a）应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除；
	要求点 b）应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。
个人信息保护	要求点 a）应仅采集和保存业务必需的用户个人信息；
	要求点 b）应禁止未授权访问和非法使用用户个人信息。

（5）安全管理中心

安全控制点	安全要求项
系统管理	要求点 a）应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；

安全控制点	安全要求项
	要求点b）应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。
审计管理	要求点a）应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；
	要求点b）应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。
安全管理	要求点a）应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计；
	要求点b）应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。
集中管控	要求点a）应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；
	要求点b）应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理；
	要求点c）应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；
	要求点d）应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求；
	要求点e）应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；
	要求点f）应能对网络中发生的各类安全事件进行识别、报警和分析。

（6）安全管理制度

安全控制点	安全要求项
安全策略	要求点a）应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。
管理制度	要求点a）应对安全管理活动中的各类管理内容建立安全管理制度；
	要求点b）应对管理人员或操作人员执行的日常管理操作建立操作规程。
	要求点c）应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。
制	要求点a）应指定或授权专门的部门或人员负责安全管理制度的制

安全控制点	安全要求项
定与发布	定；
	要求点 b）安全管理制度应通过正式、有效的方式发布，并进行版本控制。
评审和修订	要求点 a）应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。

（7）安全管理机构

安全控制点	安全要求项
岗位设置	要求点 a）应成立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权；
	要求点 b）应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；
	要求点 c）应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。
人员配备	要求点 a）应配备一定数量的系统管理员、审计管理员和安全管理员等；
	要求点 b）应配备专职安全管理员，不可兼任。
授权和审批	要求点 a）应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；
	要求点 b）应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度；
	要求点 c）应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。
沟通和合作	要求点 a）应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题；
	要求点 b）应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通；
	要求点 c）应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。
审核和检查	要求点 a）应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况；
	要求点 b）应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；
	要求点 c）应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。

（8）安全管理人员

安全控制点	安全要求项
人员录用	要求点a）应指定或授权专门的部门或人员负责人员录用；
	要求点b）应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核；
	要求点c）应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。
人员离岗	要求点a）应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；
	要求点b）应办理严格的调离手续，并承诺调离后的保密义务后方可离开。
安全意识教育和培训	要求点a）应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施；
	要求点b）应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训；
	要求点c）应定期对不同岗位的人员进行技能考核。
外部人员访问管理	要求点a）应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；
	要求点b）应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；
	要求点c）外部人员离场后应及时清除其所有的访问权限；
	要求点d）获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。

（9）安全建设管理

安全控制点	安全要求项
定级和备案	要求点a）应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；
	要求点b）应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定；
	要求点c）应保证定级结果经过相关部门的批准；
	要求点d）应将备案材料报主管部门和相应公安机关备案。
安全方案设计	要求点a）应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；
	要求点b）应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码技术相关内容，并形成配套文件；
	要求点c）应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施。
产品采购	要求点a）应确保网络安全产品采购和使用符合国家的有关规定；
	要求点b）应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要

安全控制点	安全要求项
和使用	求；
	要求点 c）应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。
自行软件开发	要求点 a)应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；
	要求点 b）应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；
	要求点 c）应制定代码编写安全规范，要求开发人员参照规范编写代码；
	要求点 d）应具备软件设计的相关文档和使用指南，并对文档使用进行控制；
	要求点 e）应保证在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测；
	要求点 f）应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制；
	要求点 g）应保证开发人员为专职人员，开发人员的开发活动受到控制、监视和审查。
外包软件开发	要求点 a）应在软件交付前检测其中可能存在的恶意代码；
	要求点 b）应保证开发单位提供软件设计文档和使用指南；
	要求点 c）应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。
工程实施	要求点 a）应指定或授权专门的部门或人员负责工程实施过程的管理；
	要求点 b）应制定安全工程实施方案控制工程实施过程；
	要求点 c）应通过第三方工程监理控制项目的实施过程。
测试验收	要求点 a）应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；
	要求点 b）应进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容。
系统交付	要求点 a）应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；
	要求点 b）应对负责运行维护的技术人员进行相应的技能培训；
	要求点 c）应提供建设过程文档和运行维护文档。
等级测评	要求点 a）应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改；
	要求点 b）应在发生重大变更或级别发生变化时进行等级测评；
	要求点 c）应确保测评机构的选择符合国家有关规定。
服务供应商选择	要求点 a）应确保服务供应商的选择符合国家的有关规定；
	要求点 b）应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务；
	要求点 c）应定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。

（10）安全运维管理

安全控制点	安全要求项
环境管理	要求点a）应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；
	要求点b）应建立机房安全管理制度，对有关物理访问、物品带进出和环境安全等方面的管理作出规定；
	要求点c）应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。
资产管理	要求点a）应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容；
	要求点b）应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；
	要求点c）应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。
介质管理	要求点a）应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；
	要求点b）应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。
设备维护管理	要求点a）应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；
	要求点b）应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等；
	要求点c）信息处理设备应经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据应加密；
	要求点d）含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用。
漏洞和风险管理	要求点a）应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补；
	要求点b）应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。
网络和系统安全管理	要求点a）应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；
	要求点b）应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；
	要求点c）应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；
	要求点d）应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；
	要求点e）应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容；
	要求点f）应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，

安全控制点	安全要求项
	及时发现可疑行为；
	要求点 g）应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库；
	要求点 h）应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据；
	要求点 i）应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道；
	要求点 j）应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为。
恶意代码防范管理	要求点 a）应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；
	要求点 b）应定期验证防范恶意代码攻击的技术措施的有效性。
配置管理	要求点 a）应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等；
	要求点 b）应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。
密码管理	要求点 a）应遵循密码相关国家标准和行业标准；
	要求点 b）应使用国家密码管理主管部门认证核准的密码技术和产品。
变更管理	要求点 a）应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施；
	要求点 b）应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程；
	要求点 c）应建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。
备份与恢复管理	要求点 a）应识别需要定期备份的重要业务信息、系统数据及软件系统等；
	要求点 b）应规定备份信息的备份方式、备份频度、存储介质、保存期等；
	要求点 c）应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。
安全事件处置	要求点 a）应及时向安全管理部门报告所发现的安全弱点和可疑事件；
	要求点 b）应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；
	要求点 c）应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训；
	要求点 d）对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。
应急预案	要求点 a）应规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容；

安全控制点	安全要求项
管理	要求点 b）应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；
	要求点 c）应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练；
	要求点 d）应定期对原有的应急预案重新评估，修订完善。
外包运维管理	要求点 a）应确保外包运维服务商的选择符合国家的有关规定；
	要求点 b）应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容；
	要求点 c）应保证选择的外包运维服务商在技术和管理方面均应具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确；
	要求点 d）应在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对 IT 基础设施中断服务的应急保障要求等。

完成上述测评工作和实施整改后，最后出具符合公安机关要求的（年度）信息系统安全保护等级测评报告。

4.安全服务

安全服务内容主要包括以下几个方面：

（1）管理制度完善

根据差距分析报告，分别从安全管理制度、安全管理机构、安全管理人员、安全建设管理以及安全运维管理五个方面确进行梳理，协助采购人制定适宜的管理制度体系文件。

（2）技术咨询与培训

按照采购人要求，提供渗透测试、风险评估、等级保护等技术咨询，及时向采购人提供最新的安全动态、技术更新和定制的安全信息。为采购人提供不少于 2 次的信息安全技术培训，确保技术人员了解、掌握关于信息系统等级保护相关规定，信息安全策略、信息保密制度，授权使用系统流程，信息安全管理制度和相关流程等。为采购方开展全方位信息安全业务培训，全面提升信息化人才队伍的安全意识和专业技能水平。

（3）信息安全巡检：服务期内为采购人每月安排技术人员对被测信息系统的安全状态进行检查并按月提供安全巡检报告。

（4）系统资产梳理

通过对系统网络拓扑结构的调查，确定各个网络安全域，分析网络拓扑结构安全；通过对资产信息的调查，确定系统中重要资产，比如服务器、核心交换机、防火墙、IDS 等；通过对服务信息的调查，确定系统服务对象；通过对系统边界的调查，确定各子系统边界情况。

（5）网络边界监测：服务期内为采购人提供有效手段监测终端计算机（windows 主机、linux 主机）、交换机等联网使用情况，确保网络运行正常。

（6）安全事件处置与应急响应：服务期内真对采购人网络和系统等具体安全事件要求进行处置与应急响应，并提供处置措施。

（7）网络病毒检测：服务期内为采购人提供有效检测手段，根据需求提供网络病毒检测结果，提供相应解决方案。

5.测评要求

在本项目 01 包验收后 15 个工作日内，须完成以下服务内容：本次测评工作需提供由公安机关颁发的三级等保备案证明，提供给采购人信息系统的安全技术测评结论、安全管

理测评结论、差距分析报告、系统安全整改方案、信息系统安全保护等级测评报告（以上材料可包含在测评报告中）；提供给采购人信息安全培训材料（包括培训课件和信息安全规范等材料）。

6、其他要求

中标方及其测评人员均要和采购人签订保密协议。

三、报价要求

本项目报总价，采购人后期不予增加任何费用，供应商须自行考虑风险。