1. **采购需求**

## 1、投标人须知前附表

|  |  |  |
| --- | --- | --- |
| 序号 | 条款名称 | 说明和要求 |
| 1 | 项目预算 | 项目总预算金额1217.02万元，本次招标金额16万元。投标人总报价不能超过采购预算，超过视为无效投标。 |
| 2 | 是否接受进口产品投标 | 接受（）不接受（√） 备注： 。 |
| 3 | 标前踏勘现场或/和标前答疑会 | 组织（）不组织（√） |
| 4 | 述标和/或产（样）品演（展）示 | 有（）无（√） |
| 5 | 投标有效期 | 从提交投标文件的截止之日起算的90天内有效。 |
| 6 | 投标要求 | 开标必须携带加密投标文件的CA数字证书、U盘和光盘内需拷贝投标文件和转换为PDF格式的盖章彩色扫描件。（或者是投标工具导出的PDF格式） |
| 7 | 评标方法 | 最低评标价法（）综合评分法（√） |
| 8 | 采购需求 | 详见采购清单 |
| 9 | 交货时间 | 详见第一章 合同履行期限 |
| 10 | 交货地点 | 用户指定地点 |
| 11 | 本项目所属行业 | 根据《统计上大中小微型企业划分办法（2017）》，本项目所属行业为软件和信息技术服务业。 |
| 12 | 备注 | 1、采购需求中未列明偏差的除特殊订制类货物以外，列明的尺寸、重量及体积允许±5%偏差。  2、采购标的物需按照国家相关标准、行业标准、地方标准或者其他标准、规范执行。  **3包要求：**  **须指导系统承建厂商按照安全相关规定达到测评合格验收标准。** |

## 

## 

## 2、采购需求

|  |  |  |
| --- | --- | --- |
| 分包名称 | | **服务内容** |
|
| **3包** | **网络安全等级保护测评服务** | 网络安全等级保护测评 |

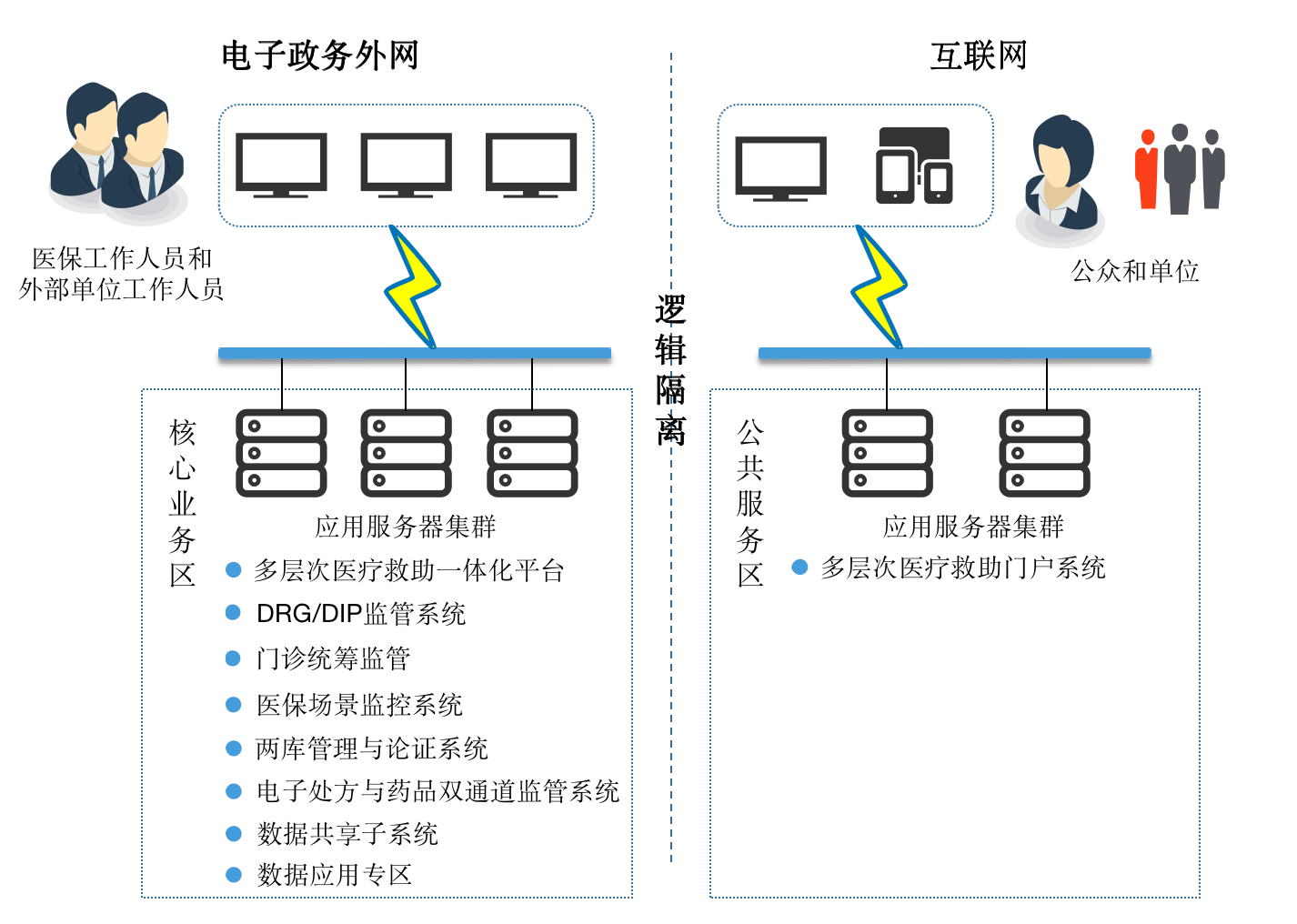
2.1项目总体概况：

按照国家医疗保障局印发的《医疗保障信息平台建设指南》要求，开展建设海南省医疗保障综合管控系统扩展和多层次医疗救助一体化平台建设项目。

核心业务区和公共服务区部署的系统如下表所示：

| **序号** | **系统** | **子系统名称** | **部署区域** | **备注** |
| --- | --- | --- | --- | --- |
| 1 | 多层次医疗救助 | 医疗救助基础信息管理系统 | 核心业务区 |  |
| 2 | 医疗救助数据共享中心 | 核心业务区 |  |
| 3 | 医疗救助业务标准规范管理系统 | 核心业务区 |  |
| 4 | 医疗救助子系统 | 核心业务区 |  |
| 5 | 应用支撑基础系统（升级） | 核心业务区 |  |
| 6 | 医疗救助门户系统 | 公共服务区 |  |
| 7 | 综合管控扩展 | DRG/DIP监管系统 | 核心业务区 |  |
| 8 | 电子处方与药品双通道监管系统 | 核心业务区 |  |
| 9 | 两库管理与论证系统 | 核心业务区 |  |
| 10 | 门诊统筹监管系统 | 核心业务区 |  |
| 11 | 医保场景监控系统 | 核心业务区 |  |
| 12 | 数据应用专区 | 数据应用专区 | 核心业务区 |  |
| 13 | 数据共享子系统 | 核心业务区 |  |

2.2海南省医疗保障综合管控系统扩展和多层次医疗救助一体化平台建设项目依托海南省政务云进行建设部署，系统部署在省国产化云计算服务平台中。业务应用子系统部署如下图所示：



2.3 信创技术路线

信息化创新是新基建的重要要求，是国家信息化建设的关键环节，是我国信息安全和产业安全的根本保障，关乎国家战略。在满足需求的情况下，各部门应积极响应当地省委省政府的信创要求，采购信创目录产品并确保系统的稳定性和可靠性。

根据海南省委、省政府的要求，新建信息化项目应按照信创国产化要求进行选购。结合国家局建设要求及海南省级医疗保障信息平台建设任务，明确了信创产品选型方案，并在后续系统建设过程中，及时跟进全国信创采购名录和适配成效而逐步完成信创产品替代工作。

2.3.1本项目软硬件选型将坚持如下原则：

2.3.1.1. 在满足信创信息化要求的前提下，保证采用国产自主可控的信创信息化设备；

2.3.1.2.在满足信创信息化要求的前提下，要充分借鉴前期试点工作经验，优先选择性能佳、兼容性好、稳定性高、适配性强、具有良好本地化保障基础和能力的产品和服务，确保系统的稳定性、可靠性；

2.3.1.3.选择符合相关标准协议的产品，确保产品间可互联互通及今后扩展；

2.3.1.4.相关安全设备选择符合相关部门认证的产品；

2.3.1.5.软件产品优先选用开放式体系架构的成熟软件产品，尽量减少自行开发工作，确保系统工作稳定；

2.3.1.6.选择低能耗的设备，优先采用一类能耗标准的获得“中国节能/环保产品”标识/证书的产品；

2.3.1.7.关键设备应支持远程管理，支持远程监控，可进行统一管理、实时监控。

2.3.2本项目信创产品选型

服务器、操作系统、数据库、中间件类

按照国家医疗保障局《关于印发医疗保障信息平台建设指南的通知》（医保网信办〔2019〕4号）要求，国家医疗保障信息平台建设遵循统一设计原则，各地在建设过程中须贯彻使用全国统一的总体、技术、业务标准规范体系及中台服务，依托全国统一的技术体系和架构，建设本地全新的医疗保障信息平台。海南省医疗保障信息平台作为国家医疗保障信息平台的重要组成部分，是践行医疗保障信息化全国“一盘棋”建设的地方实践，需严格遵循国家局建设指南要求进行建设。

2.3.2.1.本项目在服务器选型上均使用信创国产化要求的服务器。

2.3.2.2.本项目操作系统均使用信创国产要求的操作系统。其中数据中台目前基于Linux操作系统，因此需要选择支持信创架构的Linux操作系统。

2.3.2.3.由于数据库软件和中间件涉及数据同步和兼容问题，故本项目在选择数据库软件授权扩容以及中间件扩容时，按需完成国产品牌数据库及中间件进行授权扩容。另外，数据中台现有中间件组件需要进行适配，以支持信创架构，组件的实现情况需要充分考虑当前海南医保数据中台的体系架构和相关组件版本，保障业务的连续性和适配的平滑性过渡。

综上，本项目服务器、数据库、操作系统、中间件等产品尽量采用信创国产化要求产品，未包含产品采用国产品牌产品。

网络安全产品

本项目涉及网络安全产品包括防火墙、安全隔离与信息交换类、安全审计类、主机监控与审计类产品等。

本项目网络安全产品采用信创或国产化产品。

商用密码产品

本项目涉及商用密码产品包括身份认证网关、VPN网关等。

本项目商用密码产品采用信创或国产化产品，并要求使用国密算法，关键设备具备国家密码管理局颁发的商用密码产品型号证书。

本项目信创情况说明

考虑信创技术的发展，本项目中设计的服务器产品、操作系统、密码产品应充分满足信创化、合规性、安全性及高并发要求。包括但不限于：

服务器产品须为信创化产品，严格遵循国家相关管理规范和要求，入围国家信创核心目录产品或通过国家安全可靠测评。

操作系统须为信创国产要求的操作系统产品。

新建数据库入围国家信创核心目录产品或通过国家安全可靠测评，新建中间件应入围国家信创适配清单。

密码软硬件产品须为信创化密码产品，严格遵循国家密码管理规范和要求，支持国密SM2/SM3/SM4算法，符合国密安全协议和密钥管理要求。

## 3包 网络安全等级保护测评服务

一、项目概况

建设目标：

（一）加强医保监管预警机制

进一步加强对医保政策规定、服务监督工作的宣传，引导社会形成正确导向，营造全社会诚信自律、合理就医、依规提供服务、维护医疗保险基金安全、自觉抵制违约违规违法行为的社会氛围。通过汇聚内外部系统的数据和信息，提供大数据决策分析能力，支持动态化掌握全省医保制度运行情况，提供政策实施效果评估能力，根据数据模型分析与政策相融合，运用大数据智能化手段分析政策的可实施性，为海南省医保监管政策落地提供有效支撑。升级医保监管知识库和规则库，支持多库共享和规则量身订制，加强医保部门反欺诈骗保和基金监管能力。

（二）加快构筑医疗救助服务体系

依据国家医保局关于医疗保障信息平台建设的整体规划和建设指南要求和现有建设结果，结合海南省医疗保障业务需要，通过项目建设不断完善以基本医疗保险为主体、医疗救助为托底，各类补充保障制度共同发展的多层次医疗保障制度体系，通过公平普惠实施基本医疗保险、完善大病保险等补充医疗保障措施、筑牢医疗救助托底保障防线。不断提高医疗保障水平，确保医保资金合理使用、安全可控，助力推进医疗改革，更好保障人民群众就医需求、减轻医药费用负担的职责使命，着意提高新常态下全民医保制度运行公平性、基金安全性、保障可持续性、服务可及性，助力实施医疗救助，保障和改善人民群众“病有所医、病有良医”。

（三）构建监管知识规则体系新生态

以建设智慧化医保信息平台为基础，不断探索、研究、升级医保基金监管知识库和规则库内容，强化海南省医疗保障智能监管水平和基础能力。一是改变现有工作思路，发散思维逻辑，积极创新开拓医保在行业监管上的“道路”，构建全生态监测监管知识体系，知识库和规则库的建设管理要从单向的、孤立的、被动的局面逐步衍生至双向的、互动的、主动的有利环境。二是加强市县部门、各单位积极探索具有普适意义的知识信息或对应规则，同时建立动态调整机制，包括年度调整和即时调整，对出现影响“两库”适用性和有效性以及对诊疗规范、诊疗服务等出现重大调整变化时，启动即时调整程序，保障政策实施与规则建立同时落地。

（四）加强隐私数据计算安全保障

落实国家医保局要求，扎实推进医疗保障信息平台建设及运营维护，防范化解医疗保障系统数据安全风险，促进数据合理安全开发利用。实施数据全生命周期安全管理，依法依规对数据的产生、传输、存储、使用、共享、销毁等实行全生命周期安全管理，提高数据安全防护能力和个人隐私保护力度。制定统一的分级分类管理制度，按照数据分级分类保护标准、规则，对数据划分安全等级，实行分级分类管理。加强重要数据和敏感字段保护，制定重要数据保护目录，对列入目录的数据进行重点保护，涉及国家秘密、工作秘密的数据应严格保密，不予共享及公开。建立敏感数据字段库，包含但不限于个人隐私数据、参保单位隐私数据、协议机构隐私数据、药品诊疗目录项目隐私数据等。

（五）部署建设数据共享子系统

按照国家医保信息平台建设规范，统一部署建设数据共享子系统基础版本。一是建立数据目录、数据资产化管理、数据共享服务等功能，对医保海量数据进行统一在线管理。同时在保障个人隐私和公共安全的前提下，按照“原始数据不出域、数据可用不可见”的要求，向医疗保障系统外的政府部门、科研机构、第三方机构等外部单位提供数据服务，促进与外部单位的数据互联互通，满足人民群众多元化、多层次的医疗保障服务及安全保障需求。并实现对数据的使用和共享情况进行监控分析。二是实现数据专区对接工作。提高数据专区使用率，加强对市县专区的信息审核、专区审批、数据使用情况等管理工作，统一在数据共享子系统中进行管控。三是结合医保部门实际工作需要，优化并拓展数据共享子系统建设内容，提高数据管理和数据服务工作效能。

（六）发挥数据赋能场景应用价值

挖掘医保数据价值，通过统一部署数据地方专区建设，实现医保数据下沉市县，支撑各市县医保数据利用和工作开展，加强省市县纵向业务联动。建设地方专区在确保数据不出域的前提下，根据权限配置合理开放信息数据供各市县操作应用。市县医保局通过数据专区可实现参保扩面、医疗救助、区域监管、统计分析等业务开展，并利用大数据技术，提高各市县经办业务能力，助力基金监管下沉基层。建立数据隐私计算平台，融合医保数据安全、数据共享等相关机制，开发数据隐私计算工具，利用现代化、信息化手段保障隐私数据的安全性，为海南医保对数据的共享和使用提供有力支撑。

**二、建设内容**

本项目建设遵循统一设计、统一标准、统一技术架构、统一业务规范，支持横向纵向业务协同、信息共享。依据《医疗保障信息平台建设指南》，结合海南省医疗保障局实际情况，本期建设内容如下：

**综合管控系统扩展**

新一轮医改以来，医保基金监管制度体系改革持续推进，综合监管格局基本形成。综合管控系统拓展是在现有海南省医疗保障信息平台二期建设的综合管控子系统的业务架构基础上，根据本次医保改革业务需求，对综合管控子系统进行新功能增加和新模块开通，通过新技术应用进一步提高医保智能监控效能。

（一）电子处方与药品双通道监管子系统

新增电子处方与药品双通道监管系统。一是强化电子处方流转监管措施，防范欺诈骗保行为，辅助医保宏观决策。对电子处方和药品实现全过程监管，以确保药品的合法使用，提高医疗用药的安全性和透明度。二是满足统计监测需求，基于信息平台实现对电子处方、药品双通道常态化管理，加强对医保政策及标准规范的理解，持续完善监管规则，并按照现场工作做好数据统计监测分析，为智能监管体系的建设和政策引领创新提供有力支撑。

1、电子处方监管：以围绕海南省医保电子处方中心为基础，建立完善的电子处方全流程监管规则，实现对电子处方全生命周期监控，从入库、开方、流转、购药等流程上做好追踪溯源，利用数字化、自动化手段检索异常处方，并实时动态跟进处方信息，减少“药不对方”“药价偏高”等情况，利用大数据监管分析手段，增强互联网电子处方的流动性和用户使用的安全感。

2、药品双通道监管：实现对双通道药品监测、双通道药品准入、双通道药店准入进行监管，并对双通道处方用药进行审核，建立双通道处方规则知识库，实时监控处方用药全流程信息。

（二）门诊统筹监管子系统

门诊统筹监管子系统旨在提升医保门诊统筹业务的监管效能，加强对医疗机构和医保参保人员的管理和监督，确保医保资金的合理使用和医疗救助的公平执行。一是整合医保门诊统筹相关数据，通过信息技术手段实现业务流程的数字化、自动化，从而提高监管和服务水平，保障医保制度的有效运行。二是强化智能审核稽核，根据门诊统筹服务特点和运行实际，上线并逐步充实智能审核规则，扩大智能审核落实，实现对门诊统筹定点医药机构智能监控全覆盖。三是加大日常监管力度，通过智能监控、专家审核、第三方监督检查和日常巡查，全面加强门诊就医和药店购药医疗费用审核和监管。

1、规则引擎分析：建立完善门诊统筹监管规则，以“合理用药、合理检查、合理治疗、合理收费”四项工作目标为出发点，提炼门诊统筹现代化监管规则要素，完成包括但不限于门诊窜换药品及诊疗项目、违反医保药品/医用耗材和医疗服务项目目录规定等监管规则制定。实现对主要治疗药物和辅助治疗药物比例、非治疗药品和耗材监管使用占比等进行监控，充分利用规则引擎对抓取的医保业务数据进行任务调度分配和分析，实现门诊统筹业务的精细化监管。

2、风险分析与预警：汇总辖区内监管数据，对智能监管结果等信息做明细查询，为事后分析做支撑。设置风险预警阈值，对达到阈值的统筹基金总额预算、门诊共济总额预算、药品价格进行风险预警。

3、存余药量监管：实现与医保进销存接口数据对接，全量同步医院药品库存数据，同时结合“三医联动一张网”平台，通过UDI模块对药品展开溯源跟踪，完成对药品存量数据进行比对校验，提高存余药量的数据准确性，满足对辖区内患者购进、存余药品量的监管。通过大数据采集患者购药量数据，实时计算患者药品存余量，在医生开具处方时根据药品存量规则给予超量提醒，避免患者持有药品超出实际需要，减少资源浪费，规避二次销售风险。

（三）DRG/DIP监管子系统

建设DRG/DIP监管子系。一是建立医保监管服务DRG/DIP支付方式智能监控制度，实现医保DRG/DIP支付方式监管的闭环管理，提升医疗服务支付方式的管理和监管效能，确保医保基金的合理使用，增强支付的公平性和透明度。加强DRG/DIP支付方式监管保障工作，及时组建技术团队对国家医保政策、地方医保政策进行研究，并结合实际工作需要，对DRG/DIP支付方式监管内容进行调整更新，以满足海南省医疗保障基金监管整体要求，提升监管执行保障力度。二是完成与DRG/DIP支付方式系统对接联调。建立数据同步机制，通过主动推送、主动抓取等方式获取DRG/DIP支付方式全量数据，同步实现数据差异化比对工作，确保数据全部同步至监管子系统，为DRG/DIP支付方式监测监管体系提供有效支撑。

1、病案首页及结算清单质控：实现与“三医联动一张网”平台数据对接，实时抓取病案首页信息，并对数据进行查重、整理，确保病案数据分析的准确性。系统灵活配置病案首页的校验规则及分值，灵活选择校验规则的执行范围，对各医疗机构的整体病案上传数量、正确率等进行分析，并对各科室及具体病案的进行穿透分析，精准查询各病案号的错误明细，可实现医保及医疗机构快速定位问题病案及病案错误，不断提升病案首页上传质量及入组率。

2、DIP/DRG智能审核：制定针对结算清单的DIP/DRG监管规则，建立本地化的临床知识库。并对规则进行新增、停用、启用、公示等管理,并根据实际检查情况，对规则进行红橙黄的预警等级标注，重点关注预警等级较高的规则。依托于现有的智能监管系统，形成DIP违规结果初审、复审、机构申诉、申诉处理扣款执行等流程。并且可提供扣款汇总、可视化违规分析报告等内容，辅助医保基金监管决策。

3、DIP/DRG绩效考核：支持DIP/DRG绩效考核管理，通过专项指标对各医疗机构的医疗服务能力、医疗服务质量、医疗服务效率、医疗服务费用进行分析，并穿透分析各科室/MDC的医疗服务能力、医疗服务质量、医疗服务效率、医疗服务费用；对专项指标可进行权重配置，最终对医疗机构绩效考核进行排名。通过参数配置对医疗机构费率进行分类管理。

（四）两库管理与论证子系统

新增两库管理与论证子系统，进一步实现医保大数据的深度挖掘分析，持续调整、完善和创新中不断优化丰富医保两库规则，以知识库、规则库为依托，基于智慧监管系统对各类监管对象在各种场景下使用医疗保障基金的情形进行全流程监控，进一步健全医疗保障基金监管体系，提升监管效能，促进基金有效使用。建立医保规则迭代生态环境，引入第三方、专家团队等医保行业领域人才，持续开展挖掘医保反欺诈、飞行检查、智能监管等规则体系，探索医疗保障行业市场可行性监管手段，输出“事前精准干预”有效办法，结合大数据引擎计算和智能化信息系统，从源头上保护医疗保险基金安全可控。

两库论证服务：依托于两库管理系统，不定期开展对医保监管规则库、知识库的研究探索，引入第三方、行业专家等对规则内容进行评审，确保符合医保政策和监管要求。

两库生态环境：发挥海南省医保智能监管优势，挖掘各地、各单位以及兄弟省份知识库、规则库行业动态，构建省市县纵向联动机制，建立健全医保全业务全流程全场景监管模式，创新海南省医保两库生态发展环境。

（五）医保场景监控系统

建立和完善医保智能监控系统，加强大数据应用。依托视频监控、生物特征识别等技术应用，保障医保基金监督，打击欺诈骗保等行为，实现监管关口前移，丰富监管维度，精准医保监管，提升监管效能。同时，对医院、药店等场景需采购的设备做统一接入要求，明确硬件设备由地方自行采购，并且需要满足医保接入标准。医保场景监控系统主动采集数据，实时开展智能监控常态化，综合应用医疗保障智能监控和大数据分析手段，实现线索发现、调查取证、违规处理、结果应用等监管环节线上线下相结合，形成全流程闭环监管。建立硬件设备监控管理功能，对接入设备的信息、型号、规格等进行统一查询、统一维护、统一管理，并实时监控设备运行使用状况，及时同步设备维护信息，确保两定机构设备正常运行。

1、采集端：通过两定机构部署的硬件设备，采集相关场景数据包括门诊、住院、血透等，采集内容为住院信息、门诊信息、血透信息、人脸图像、视频等。

2、监管端：通过采集端收集数据，利用知识规则库和大数据模型计算，主动发现异常就医行为数据并挖掘可疑信息，产出统计分析结果。

3、机构端：为两定机构提供信息核查入口，对不同场景的患者进行身份识别、在院/住院查询、购药信息查询等功能。

4、视图库管理端：提供可视化展示，实现包括视频、图像等查看界面，并对接入的硬件设备进行统一在线管理。

5、移动稽核：移动稽核主要有稽核处理、远程查房、申诉审核、信息查询、门诊住院血透购药场景大数据分析等功能，可实现对门诊、住院、血透、药店四个场景稽核任务下达，远程查床任务下达，稽核问题申诉处理，四个场景的患者信息查询，及四个场景的大数据分析。

6、系统支撑：提供统一系统管理功能，实现对基础信息、就诊信息的同步。可对接入设备进行查看、导出。实现系统用户信息、算法参数等维护工作。

**多层次医疗救助一体化平台建设**

（一）多层次医疗救助门户系统

多层次医疗救助门户系统提供全面的医疗救助服务，促进救助对象获得合理、有效的医疗救助。一是构建医疗救助公共服务窗口，为救助群体提供一站式服务，通过APP、公众号、小程序等互联网产品，打通医疗救助申请渠道，减轻救助群体线下提交的压力和困难，利用现代化、电子化技术保障救助申请便利便捷。同时对接海易办、政务一体化平台，为推动海南省“医疗救助一件事一次办”提供有效支撑。二是接入海政通用户账户信息，避免基层服务人员重复记录账户，只需使用海政通账号密码即可访问医疗救助门户系统，即可开展对救助人员的信息审核工作。三是做好技术保障工作，通过后台管理审核人员权限信息，及时开通、收回相关权限，加强对人员的管理工作，避免出现救助信息审核慢、救助信息审核有误等情况。

用户救助申请：以自动化申请为建设目标，减少群众输入重复信息、无用信息等。与医保二期平台、三医联动平台以及横向单位系统实现数据互通，自动获取救助人员相关信息，包括救助对象基本情况、参保情况、就医结算、诊疗处方等数据。逐步替换线下纸质版填报申请流程，实现救助服务平台智能化应用，为社会底层人员、文化弱势群体提供更便捷、更人性化的多层次医疗救助一站式服务。

接入海政通账户信息：通过获取海政通用户身份信息，将账户信息自动同步到多层次医疗救助门户中，便于业务人员登录信息系统，减少账号开通步骤。同时按照海政通组织架构及权限管理模式，即时同步更新用户账户信息，对不用的账户进行注销，确保人员离职、人员调动后的相关账号权限收回，防止发生信息泄露以及违规审批等风险。

（二）多层次医疗救助数据共享中心

多层次医疗救助数据共享中心主要实现将各救助单位业务专网整合至全省电子政务外网，推进分散的、独立的信息系统整合为一个互联互通、信息共享、业务协同的“大系统”。以围绕建立“一个平台、两个池子、三个机制”为目标，利用数据中心共享机制，开展与省民政厅、省卫健委、省总工会、省乡村振兴局、省残联、省妇联、省团委、省退役军人事务局、红十字会、慈善等13家单位以及后续接入部门的系统对接联调工作，确保数据共享机制平稳运行。同步接收医疗救助门户、横向救助部门数据信息，开展医疗救助信息审核、救助身份认定、救助身份标识、医疗救助资金核算等业务，主动将相关救助信息推送至各救助部门，做到数据互联互通、救助信息有效链接，防止出现救助不足、救助信息差异化等情况。同时，通过数据共享中心可实现查看救助对象的医疗救助情况，包括救助时间、救助费用、救助单位等，为部门政策决策提供有效支撑。

1、数据接入：一是可通过省大数据局数据共享交换中心进行数据申请，由大数据局推送数据至多层次医疗救助数据共享中心。二是实现与横向单位系统接入，通过API接口、库表等方式，打通多部门系统与多层次医疗救助数据共享中心互联互通，提高数据传送效率。

2、横向单位接入：构建多层次医疗救助一体化服务机制，与13家救助单位以及后续接入单位做好接口对接工作。承建单位主导开发、测试、联调相关接口，并输出接口对接文档，确保系统接入无异常，同时负责接口更新维护工作，为13家救助单位以及后续接入单位对接做好技术保障。

3、一站式结算：系统建设预留一站式结算接入方式，为实现全省统一一站式救助提供实施路径。基于医保报销、大病报销后个人支付费用，以救助政策为导向，探索医疗救助一站式结算统筹支付模式，减轻老百姓垫付压力，让老百姓能真正意义上感受到多层次医疗救助一体化服务的人性化、便利性。

（三）应用支撑基础系统升级

应用支撑基础系统实现对整个业务应用系统运行的基础配置和支撑功能，通过对原有子系统进行升级改造，用以支撑多层次医疗救助一体化平台的业务开展和医疗救助信息及相关数据的互通共享。同时需满足医保数据内部使用需要，对医疗救助信息实现同步，为公共服务、宏观决策分析、大数据分析预警等业务系统做好基础支撑工作。

（四）多层次医疗救助业务标准规范管理系统

建设多层次医疗救助业务整体元数据标准、数据集标准、数据共享标准、接口标准、数据治理规范等整体管理系统，为构建全省统一的多层次医疗救助数据交换与共享中心提供支撑和依据。系统建设包括但不限于对数据的定制化治理工作，为支撑多层次医疗救助一体化平台有效开展，建立起专项的医疗救助数据标准团队，提供常态化治理工作。并且需要满足横向救助单位的数据使用需求，做好数据标准对接沟通工作，及时响应相关单位，输出医保数据标准及编码对照，建立完善的多层次医疗救助数据标准综合体系。

业务数据标准服务：建立海南省多层次医疗救助数据标准化服务，满足各单位在共享医疗救助数据的标准对照映射，同时以医保救助数据标准为基础，实现多层次医疗救助数据标准基础版本，并为各救助单位提供标准化技术服务支撑，推动多层次医疗救助一体化、标准化建设。

业务数据安全保障：建立多层次医疗救助数据安全保障团队，提高数据在标准化、治理化过程中的安全响应工作，增强多层次医疗救助数据标准综合服务保障能力，减少数据在转码、治理、归集和使用过程中出现数据丢失和泄露等情况。

（五）医疗救助子系统升级

基于海南省医疗保障统筹救助模式，发挥医保救助整体水平和能力，将医疗救助模块进行独立应用，建立医疗救助子系统，为业务经办提供平台支撑。整体建设内容包括但不限于医疗救助拨付管理、医疗救助对象管理、医疗救助信息查询等，并结合医保局、医保服务中心工作需要，开展对城乡医疗救助情况、城乡居民基本医疗保险缴费和财政补助情况等查询统计，形成相关报表内容，供医保工作人员调阅、导出等，并根据业务部门要求，对报表内容进行定制化开发，方便工作人员对数据进行分析研究。

与多层次医疗救助一体化平台对接：满足业务开展需要，实现与多层次医疗救助一体化平台对接，实时同步包括民政救助、妇联救助、残联救助等数据信息。

与财务系统对接：通过与财政财务系统的对接，获取医疗救助资金、财政补助情况等，为确保医保部门、经办机构实现医疗救助情况摸底和统计提供数据支撑能力。

（六）多层次医疗救助基础信息管理系统

多层次医疗救助基础信息管理系统有效管理和维护与医疗救助对象相关的信息。该系统涵盖了从信息收集、存储到查询分析等全过程。有助于提高医保、民政、乡村振兴、残联、妇联、总工会、慈善、红十字等13家单位救助工作的效率和质量，更好地满足医疗救助对象管理的需求，为政府部门和救助机构提供科学依据，促进医疗救助工作的规范和透明。同时，通过系统的数据分析和监测，可以不断优化救助政策，提升公共服务水平，为需要医疗救助的人群提供更加精准和周到的支持。

**部署数据共享子系统**

按要求部署国家医保局下发的数据共享子系统，建立数据共享工作机制，为提高医保业务横纵向联动提供平台支撑，同时实现与医保二期平台业务系统、业务中台、数据中台以及数据专区完成对接，提升数据共享子系统核心功能价值。一是加强海南省医保数据日常管理，建立数据目录、数据共享、数据资产等管理功能，提升医保数据可查、可管、可控。二是通过数据内外共享，增强医保综合业务能力，提升经办、监管、决策、药招等数据使用效能，打通医保与政务信息化业务信息壁垒，解决数据共享障碍。二是打通与数据专区有效衔接，利用数据共享子系统实现对专区的统一管理，由省医保局接收各市县提交的专区任务申请，并结合实际工作场景分发对应的权限，以确保各市县能精准化获取相关数据。同时对数据专区使用情况做好统计监测，实时动态掌握全域数据使用情况，避免发生数据泄露、丢失、异常导出等行为，提高数据安全防护力度。

部署升级及应用开发：完成国家数据共享子系统后续升级更新工作，并结合省市地方需求，对海南省数据共享子系统模块进行个性化开发，以满足实际业务开展需要。

数据共享子系统业务保障：负责对数据共享子系统日常管理工作，完成包括但不限于数据目录维护升级、数据共享管理、数据资产管理、数据专区管理数据审计管理等。

**数据专区**

（一）数据提取

为满足市县数据使用需要，在建立数据地方专区后，由开发团队将各市县对应的数据进行提取，完成对市县专区的数据同步工作，并结合数据更新周期，实现数据增量同步功能，确保各市县掌握医保全量数据。同时根据国家医保局、省医保局相关办法规定，对数据进行分类分级，以满足市县在获取数据后能快速掌握信息的整体情况和安全等级。同时做好数据提取保密和保护工作，数据抽取和推送需要做到信息隔离，坚持“谁的数据谁使用”原则，对未通过数据共享子系统申请的数据请求工作一律不予受理，从数据提取工作中把好第一关，保障数据分发安全可控。

（二）数据开发

市县医保部门通过数据地方专区，实现医保数据再开发、再利用，通过建立不同业务的应用场景，加强市县横纵向数据交换，提升包括多层次医疗救助、大数据反欺诈、飞行检查、支付方式监管等业务联动，丰富各市县医保大数据服务能力。同时结合数据开发过程，持续对原数据的治理和清洗工作，市县医保部门须按照国家医保局、省医保局数据治理有关办法，建立起数据质控体系，对医保目前存留的脏数据做到全面治理，提升海南医保综合服务质量。

（三）数据安全沙箱

在数据专区中设置数据安全沙箱，在不暴露真实数据的情况下进行数据分析和共享。数据沙箱提供安全防护的能力，允许多个实体共享数据，同时保持数据的隐私和安全。在数据沙箱中，数据被匿名化或脱敏处理，使得数据所有者的敏感信息得到保护。在数据安全沙箱中实现对专区的全员全业务全流程监测监管，提高数据专区安全保障，保障数据安全事件进行有效预警和溯源。

1、隐私计算：在数据沙箱中，通过隐私计算引擎对数据实现脱敏加密，以避免直接暴露个人敏感信息。确保数据在共享过程中不会泄露隐私。

2、数据分割：通过后台权限配置，数据沙箱可以将数据分割成不同的部分，使得不同用户只能访问特定的数据片段。减少数据泄露的风险。

3、加密保护：数据沙箱可以使用加密技术来保护数据的传输和存储过程，防止未经授权的访问和窃取。

4、安全审计：提供安全沙箱审计能力，通过细粒度的数据管理策略，构建数据安全空间和审计管理空间，实现沙箱内的数据流转可管可控可审计。

（四）数据运营

构建医保数据运营中心，支撑数据专区常态化运行，利用大数据监测手段实时掌握全省专区应用情况。一是在系统功能和日常管理上实现专区全员全业务全流程监测，建设完善监管规则，对异常行为账户做到“提前预警，快速干预”，必要时将自动暂停账户使用的权限，确保数据不被窃取。二是利用可视化掌握专区资源状况，展示全省各地数据专区使用的状况，并合理对资源进行分配，加强对热度专区的基础保障，减少专区资源浪费。三是加强日常保障工作，对数据地方专区应用进行巡检测试，保障专区平稳运行。同时做好台账记录，对专区使用、开发、数据导出、数据治理等做好日志留存，提升数据运营价值。四是定期产出运行分析报告，包括但不限于完成数据专区使用情况报告、数据沙箱运行分析报告、资源资产化评估报告、数据专区安全审计报告等。

**平台总体架构**

本项目建设承继现有海南省医疗保障信息平台的总体架构，严格按照国家医疗保障信息平台建设指南的相关约束与要求，遵循国家医疗保障信息平台的统一设计原则，贯彻全国统一的标准规范体系和中台服务架构，依托全国统一的技术框架完成系统建设。



**图 总体架构图**

（一）展现层

核心业务区入口：通过内部统一门户面向全省工作人员提供统一的核心业务区系统访问入口，实现全省人员在医疗保障信息平台的单点登录和统一身份认证，同时通过内部统一门户接收医疗保障信息平台的消息提醒并处理自身日常工作的各类待办事务。

公共服务区入口：通过个人网厅、企业网厅、APP及自助终端等面向执业人员、医疗机构、社会公众和企业提供医保业务的办理、查询、咨询、监督等渠道；药品和医用耗材招采管理模块为药品和医用耗材招采提供访问入口。

（二）应用层

核心业务区中的生产区应用系统：包括业务经办子系统、综合管控子系统、支付方式管理子系统、应用支撑子系统。新建多层次医疗救助平台，实现海南省医疗救助一体化对接；部署国家下发的数据共享子系统，建立健全医保数据共享机制和共享模式。

核心业务区中的大数据区应用系统：智慧决策子系统，通过大数据服务及在线分析数据库、离线分析数据库作为数据应用场景的支撑；数据专区，通过数据推送，建立数据开发中心、隐私计算中心、可视化中心和运营中心。

公共服务区中的应用系统：公共服务子系统，包括公共服务模块和药品医用耗材招采两个模块；医疗救助门户系统，实现多层次医疗救助公共服务业务开展，提供多端申请入口，例如海南医保APP、公众号、小程序等。

（三）政务中台层

政务中台包括业务中台和数据中台，对应用系统提供服务逻辑支撑。核心业务中台抽取各系统间可共享、可复用的业务能力，形成共享业务中心。应用层的各应用系统通过调用核心业务中台所提供的各业务中心中台服务，并要应用层进行逻辑组装和业务实现。最大程度地提升系统间协作效率，实现核心业务系统高弹性、高容错的技术特点。同时，服务层提供了数据中台，实现数据计算和分析服务，并且完成数据的综合治理。

数据中台基于数据资源池提供数据综合治理服务和数据计算服务。数据综合治理服务通过数据可视化、数据管理、数据开发等手段构建平台数据综合治理服务能力，实现数据的深度综合治理。数据计算服务通过构建各类数据计算服务能力，搭建机器学习、深度学习、分析预测、决策、计算框架等计算服务能力，为上层业务系统进行数据处理、数据计算、数据分析提供能力保障

核心业务区数据中台包括了两大能力：

1．数据综合治理能力，完成数据的整合、转换、清洗及数据质量处理，并实现专题数据的生产能力；

2．大数据价值挖掘能力，通过定义数据应用场景，构建模型，并进行训练和计算，挖掘大数据价值，为新业务及政策优化提供数据依据。

（四）支撑层

支撑层包括了核心业务区中的交换区所提供的共享交换支撑平台能力，并且提供适配器，以及可加载的第三方分布式中间件、工具、产品或应用。

核心业务区中交换区：

交换区主要基于数据中台支撑数据交换库以及共享交换平台的建设，以实现海南医保平台横向与海南省数据交换平台和纵向与国家局平台的数据共享与交换。

适配器：

适配器包括核心业务区适配器和公共服务区适配器，是为了实现分布式中间件与产品服务与业务中台之间的技术解耦而建立，负责服务第三方分布式中间件、工具、产品或应用的注册、对象引用的创建和解释、对象实现的激活和去活以及客户请求的分发等。

（五）分布式中间件及产品服务

为上层应用系统提供各类基础能力支持，包括：

1．业务支撑类服务组件

业务支撑服务组件是针对医疗保障信息平台所需的各项服务能力。业务支撑服务组件所包含用于进行数据交换的业务网关、用于进行消息接收的即时消息、用于进行对账操作的对账服务组件等。

2．基础服务支撑组件

基础服务支撑组件是通过整合系统运行时所需的各项服务能力提供统一的功能服务。基础服务支撑组件提供的基础服务功能包括数据采集、二维码管理、站内消息、邮件服务、生物识别和密码管理。

3．中间件

中间件是一种独立的系统软件或服务程序，分布式应用软件借助中间件在不同的技术之间共享资源。中间件包括业务通用服务组件、大数据分析组件。

（六）基础设施层

构建计算、存储、网络资源池，提供计算服务、存储服务和网络服务。

（七）安全运维体系

针对医疗保障信息平台进行安全防护体系建设，并制定相关信息化标准体系指导信息化整体项目的推进工作，同时制定运维体系保证信息化业务系统及硬件设施后期的安全稳定运行。其中安全防护体系内容包括网络安全技术体系、网络安全管理体系和网络安全运营体系；运维管理体系主要包括运维管理平台、运维服务体系、运维组织体系、运维管理制度体系、运维管理考核指标。

**技术要求**

服务内容：

（1）信息系统安全等级保护测评

根据《信息安全技术网络安全等级保护基本要求》（GB/T 22239一2019）的相关法律和技术标准要求，对海南省医疗保障综合管控系统扩展和多层次医疗救助一体化平台建设项目内的2个业务系统（13个子系统）：分别是多层次医疗救助一体化服务平台和数据专区（多层次医疗救助基础信息管理系统、多层次医疗救助数据共享中心、多层次医疗救助业务标准规范管理系统、应用支撑基础系统、医疗救助子系统、多层次医疗救助门户系统、数据共享子系统、数据专区）；综合管控系统拓展和医保场景监控（电子处方与药品双通道监管、DRG/DIP监管系统、门诊统筹监管、两库管理与论证系统、医保场景监管系统）进行安全等级保护测评工作。

**具体内容应包括：**

1）完成信息系统定级备案工作，协助招标方完成信息系统多层次医疗救助一体化服务平台和数据专区和综合管控系统拓展和医保场景监控等保三级定级备案工作。

2）海南省医疗保障综合管控系统扩展和多层次医疗救助一体化平台建设项目内的所有系统进行安全等级保护测评。测评内容包括物理安全、网络安全、主机安全、应用安全、数据安全及备份、安全管理。客观地分析这些信息系统安全保护现状和信息安全等级保护基本要求之间的差距。

3）协助招标方进一步完善等级保护管理体系。根据《信息安全等级保护管理办法》和《信息安全技术网络安全等级保护基本要求》，结合测评的结果，协助招标方进一步完善信息安全等级保护管理体系。

4）协助招标方进一步完善等级保护安全技术措施。结合等级保护测评报告提出的安全防护现状与等级保护基本要求之间的差距，明确安全需求，设计符合相应等级要求的信息系统安全技术建设整改方案。

5）完成测评备案工作。在完成上述信息系统安全等级保护测评工作的基础上，提交这些系统的测评报告至公安局等保办，最终完成测评备案工作。

6）对测评过程检测出来的高危漏洞，须提供有效的解决方案并帮助相应系统的管理员完成整改。对于确认无法完成的整改，须提供书面证明。

**网络安全测评原则**

网络安全测评方案设计与实施应满足以下原则：

符合性原则：应符合国家信息安全等级保护制度及相关法律法规，指出防范的方针和保护的原则。

标准性原则：方案设计、实施与信息安全体系的构建应依据国内、国际的相关标准进行。

规范性原则：项目实施应由专业的等级测评师依照规范的操作流程进行，在实施之前将详细量化出每项测评内容，对操作过程和结果提供规范的记录，以便于项目的跟踪和控制。

可控性原则：项目实施的方法和过程要在双方认可的范围之内，实施进度要按照进度表进度的安排，保证项目实施的可控性。

整体性原则：安全体系设计的范围和内容应当整体全面，包括安全涉及的各个层面，避免由于遗漏造成未来的安全隐患。

最小影响原则：项目实施工作应尽可能小的影响网络和信息系统的正常运行，不能对信息系统的运行和业务的正常提供产生显着影响。

保密原则：对项目实施过程获得的数据和结果严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据和结果进行任何侵害测评委托单位利益的行为。

**网络安全测评依据**

信息系统等级测评依据《信息系统安全等级保护基本要求》、《信息系统安全等级保护测评要求》，在对信息系统进行安全技术和安全管理的安全控制测评及系统整体测评结果基础上，针对相应等级的信息系统遵循的标准进行综合系统测评，提出相应的系统安全整改建议。

主要参考标准如下：

《计算机信息系统安全保护等级划分准则》-GB17859-1999

《信息安全技术信息系统安全等级保护实施指南》

《信息安全技术信息系统安全等级保护测评要求》

《信息安全等级保护管理办法》

《信息安全技术信息系统安全等级保护定级指南》（GB/T22240-2008）

《信息安全技术信息系统安全等级保护基本要求》（GB/T22239-2019）

《计算机信息系统安全保护等级划分准则》（GB17859-1999）

《信息安全技术信息系统通用安全技术要求》（GB/T20271-2006）

《信息安全技术网络基础安全技术要求》（GB/T20270-2006）

《信息安全技术操作系统安全技术要求》（GB/T20272-2006）

《信息安全技术数据库管理系统安全技术要求》（GB/T20273-2006）

《信息安全技术服务器技术要求》（GB/T21028-2007）

《信息安全技术终端计算机系统安全等级技术要求》（GA/T671-2006）

《信息安全风险评估规范》（GB/T20984-2007）

**网络安全测评流程**

**1）测评准备阶段**

测评项目组组建：明确主管责任人、测评人员及职责分工。

项目计划书编制：项目计划书包含项目概述、工作依据、技术思路、工作内容和项目组织等。

信息系统调研：通过查阅被测系统已有资料或使用调查表格的方式，了解整个系统的构成和保护情况，明确被测系统的范围（特别是信息系统的边界），了解被测系统的详细构成，包括网络拓扑、业务应用、业务流程、设备信息（服务器、数据库、网络设备、安全设备、数据库等）、管理制度等。

工具和表单准备：根据被测系统的实际情况，准备测评工具和各类测评表单。

**2）方案编制阶段**

测评对象确定：根据已经了解到的被测系统信息，分析整个被测系统及其涉及的业务应用系统，确定出本次测评的测评对象。

测评指标确定：根据已经了解到的被测系统定级结果，确定出本次测评的测评指标。

测评工具接入点确定：确定需要进行工具测试的测评对象，选择测试路径，根据测试路径确定测试工具的接入点。

测评内容确定：确定现场测评的具体实施内容，即单元测评内容。

测评实施手册开发：编制测评实施手册，详细描述现场测评的工具、方法和操作步骤等，具体指导测评人员如何进行测评活动。

**3）现场测评阶段**

现场测评实际上就是单项测评，分别从技术上的安全物理环境、安全通信网络、安全计算环境、安全区域边界和安全管理中心五个层面和管理上的安全建设管理、安全管理人员、安全管理制度、安全管理机构和安全运维管理五个方面分别进行。

安全物理环境：通过人员访谈、文档审查和实地察看的方式测评信息系统的安全物理环境保障情况。主要涉及对象为物理基础设施。在内容上，安全物理环境层面测评实施过程涉及10个测评单元，包括：物理位置的选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护。

安全通信网络：通过访人员访谈、配置检查和工具测试的方式测评信息系统的安全通信网络保障情况。主要涉及对象为网络互联设备、安全通信网络设备和网络拓扑结构。在内容上，安全通信网络层面测评实施过程涉及7个测评单元，包括：结构安全、访问控制、安全审计、边界完整性检查、入侵防范、网络设备防护、恶意代码防范（针对三级系统）。

主机安全：通过人员访谈、配置检查和工具测试的方式测评信息系统的主机安全保障情况。主要涉及对象为各类服务器的操作系统、数据库管理系统。在内容上，安全计算环境层面测评实施过程涉及7个测评单元，包括：身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、资源控制、剩余信息保护（针对三级系统）。

安全区域边界：通过人员访谈、配置检查和工具测试的方式测评信息系统的安全区域边界保障情况，主要涉及对象为各类应用系统。在内容上，安全区域边界层面测评实施过程涉及9个测评单元，包括：身份鉴别、访问控制、安全审计、通信完整性、通信保密性、软件容错、资源控制、剩余信息保护（针对三级系统）、抗抵赖（针对三级系统）。

安全管理中心：通过人员访谈、配置检查的方式测评信息系统的安全管理中心保障情况，主要涉及对象为信息系统的管理数据及业务数据等。在内容上，安全管理中心层面测评实施过程涉及3个测评单元，包括：数据完整性、数据保密性、备份和恢复。

安全管理人员：通过人员访谈、文档审查和实地察看的方式测评信息系统的安全管理人员情况。在内容上，安全管理人员方面测评实施过程涉及3个测评单元，包括：管理制度、制定和发布、评审和修订。

安全建设管理：通过人员访谈、文档审查的方式测评信息系统的安全建设管理情况。在内容上，安全建设管理方面测评实施过程涉及5个测评单元，包括：岗位设置、人员配备、授权和审批、沟通和合作、审核和检查。

安全管理制度：通过人员访谈、文档审查的方式测评信息系统的安全管理制度情况。在内容上，安全管理制度方面测评实施过程涉及5个测评单元，包括：人员录用、人员离岗、人员考核、安全意识教育和培训、外部人员访问管理。

安全管理机构：通过人员访谈、文档审查的方式测评信息系统的安全管理机构情况。在内容上，安全管理机构方面测评实施过程涉及11个测评单元，包括：系统定级、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、安全服务商选择、系统备案（针对三级系统）、系统测评（针对三级系统）。

安全运维管理：通过人员访谈、文档审查的方式测评信息系统的安全运维管理情况。在内容上，安全运维管理方面测评实施过程涉及13个测评单元，包括：环境管理、资产管理、介质管理、设备管理、安全通信网络管理、系统安全管理、恶意代码防范管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理、监控管理和安全管理中心（针对三级系统）。

**4）分析与报告编制阶段**

单项测评结果分析：针对测评指标中的单个测评项，结合具体测评对象，客观、准确地分析测评证据。

单元测评结果判定：将单项测评结果进行汇总，分别统计不同测评对象的单项测评结果，从而判定单元测评结果，并以表格的形式逐一列出。

整体测评：针对单项测评结果的不符合项，采取逐条判定的方法，从安全控制间、层面间和区域间出发考虑，给出整体测评的具体结果，并对系统结构进行整体安全测评。

风险分析：据等级保护的相关规范和标准，采用风险分析的方法分析等级测评结果中存在的安全问题可能对被测系统安全造成的影响。

等级测评结论形成：在测评结果汇总的基础上，找出系统保护现状与等级保护基本要求之间的差距，并形成等级测评结论。

测评报告编制：根据等级测评结论，编制测评报告，包括概述、被测系统描述、测评对象说明、测评指标说明、测评内容和方法说明、单元测评、整体测评、测评结果汇总、风险分析和评价、等级测评结论、整改建议等。

**网络安全测评方法**

在等级保护测评过程中，将采用以下测评方法：

**1）工具测试**

利用技术工具（漏洞扫描工具、渗透测试工具、压力测试工具等）对系统进行测试，包括基于网络探测和基于主机审计的漏洞扫描、渗透测试等。

表2网络安全测评方法-工具测试

|  |  |
| --- | --- |
| **测评方法** | **工具测试** |
| **简要描述** | 利用技术工具，从网络的不同接入点对网络内的主机、服务器、数据库、网络设备、安全设备等进行脆弱性检查和分析 |
| **达成目标** | 发掘系统的安全漏洞 |
| **工作条件** | 1-2人工作环境，电源和网络接入环境，用户、网络、系统配合 |
| **工作结果** | 工具测试结果记录 |

**2）配置检查**

利用上机验证的方式检查主机、服务器、数据库、网络设备、安全设备、应用系统的配置是否正确，是否与文档、相关设备和部件保持一致，对文档审核的内容进行核实（包括日志审计等），测评其实施的正确性和有效性，检查配置的完整性，测试网络连接规则的一致性，从而测试系统是否达到可用性和可靠性的要求。

表3网络安全测评方法-配置检查

|  |  |
| --- | --- |
| **测评方法** | **配置检查** |
| **简要描述** | 通过登录系统控制台的方式，人工核查和分析主机、服务器、数据库、网络设备、安全设备、应用系统的安全配置情况 |
| **达成目标** | 发现配置的安全隐患 |
| **工作条件** | 1-2人工作环境，用户、网络、系统配合 |
| **工作结果** | 配置检查结果记录 |

**3）人员访谈**

与被测系统有关人员（个人/群体）进行交流、讨论等活动，获取相关证据，了解有关信息。在访谈范围上，不同等级信息系统在测评时有不同的要求，一般应基本覆盖所有的安全相关人员类型，在数量上可以抽样。

表4网络安全测评方法-人员访谈

|  |  |
| --- | --- |
| **测评方法** | **人员访谈** |
| **简要描述** | 通过交流、讨论的方式，对技术和管理方面进行脆弱性检查和分析 |
| **达成目标** | 发掘技术和管理方面存在的安全问题 |
| **工作条件** | 1-2人工作环境，用户配合 |
| **工作结果** | 人员访谈结果记录 |

**4）文档审查**

检查制度、策略、操作规程、制度执行情况记录等文档（包括安全方针文件、安全管理人员、安全管理的执行过程文档、系统设计方案、网络设备的技术资料、系统和产品的实际配置说明、系统的各种运行记录文档、机房建设相关资料、机房出入记录等过程记录文档）的完整性，以及这些文件之间的内部一致性。

表5网络安全测评方法-文档审查

|  |  |
| --- | --- |
| **测评方法** | **文档审查** |
| **简要描述** | 通过文档审核与分析，检查制度、策略、操作规程、制度执行情况记录的完整性和内部一致性 |
| **达成目标** | 发掘技术和管理方面存在的安全问题 |
| **工作条件** | 1-2人工作环境，用户、各类文档资料配合 |
| **工作结果** | 文档审查结果记录 |

**5）实地查看**

通过实地的观察人员行为、技术设施和物理环境状况判断人员的安全意识、业务操作、管理程序和系统物理环境等方面的安全情况，测评其是否达到了相应等级的安全要求。

表6网络安全测评方法-实地查看

|  |  |
| --- | --- |
| **项目名称** | **实地查看** |
| **简要描述** | 通过现场查看人员行为、技术设施和物理环境状况，检查人员的安全意识、业务操作、管理程序和系统物理环境等方面的安全情况。 |
| **达成目标** | 发掘技术和管理方面存在的安全问题 |
| **工作条件** | 1-2人工作环境，甲方人员配合 |
| **工作结果** | 实地查看结果记录 |

**6）网络安全测评工具**

在等级保护测评过程中使用的测评工具严格遵循可控性原则，即所有使用的测评工具将事先提交进行检查确认，确保在双方认可的范围之内，而且测评过程中采用的技术手段确保已经过可靠的实际应用。

**7）输出文档**

本项目测评输出的主要输出文档为：

《等级保护测评实施方案（资产收集、测评表）》

《等级保护测评差距分析报告》

《等级保护测评安全整改方案》

《等级保护测评安全整改报告》

**8）时间安排**

表7网络安全测评时间安排

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **任务名称** | **工作内容** | **阶段完成标志** |
| 1 | 项目准备阶段 | 编制实施方案 | 《实施方案》 |
| 2 | 编制资产收集 | 资产收集表 |
| 3 | 编制测评表 | 测评表 |
| 4 | 前期调研 | 资产收集 | 完成  资产收集表 |
| 5 | 差距测评 | 技术和管理单项测评 | 完成信息  系统测评表 |
| 6 | 差距测评报告编制 | 单元测评、整体测评、风险分析、报告编制 | 《差距测评报告》 |
| 7 | 安全整改建议 | 对部分风险较高的不符合项给出整改报告 | 《整改方案》 |
| 8 | 安全加固与检查 | 对整改部分内容进行复检 | 《整改报告》 |
| 9 | 等级保护验收测评 | 协助中心通过第三方测评 | 获得测评证书 |

**人员安排**

**工作分工**

为确保网络安全测聘工作顺利进行，将于服务商协商组建项目测评小组，并对组织机构如下规划。

表8网络安全测评-工作分工

|  |  |
| --- | --- |
| **名称** | **职责** |
| 项目负责人 | 项目总体负责人，负责组织等级保护测评和评估实施队伍，做好整体日常资源管理、分配与协调工作，并直接控制整体项目管理的各个要素，具体包括：  项目方案设计  项目计划与组织  项目协调与沟通（含召集项目周例会）  项目进度管理（含编写项目周报）  项目质量控制 |
| 项目  技术人员 | 项目技术人员，包括项目分组组长和实施人员，在项目经理的带领、分工和控制下，负责按照项目技术方案和项目计划实施测评和评估工作，需要提交：  每天工作日报  单项测评结果记录  单项安全整改建议 |

**人员配置表**

网络安全测评-人员配置表

|  |  |  |
| --- | --- | --- |
| **名称** | **职责** | **人员** |
| 项目  负责人 | 项目总体负责人，负责组织等级保护测评和评估实施队伍，做好整体日常资源管理、分配与协调工作，并直接控制整体项目管理的各个要素，具体包括：  项目方案设计  项目计划与组织  项目协调与沟通（含召集项目周例会）  项目进度管理（含编写项目周报）  项目质量控制 | 1人 |
| 项目  技术人员 | 负责按照项目技术方案和项目计划实施测评工作，需要提交：  每天工作日报  单项测评结果记录  单项安全整改建议 | 每个测评项不少于2人 |

**工作配合**

为保证本项目的顺利实施，对现场测评阶段的各项工作点提出与服务商工作配合：

表9网络安全测评-工作配合

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **工作点** | **前期准备** | **服务商配合** |
| 1 | 现场工具测评 | 1、人员要求  系统管理员  \*前期提供系统软硬件配置，相关系统检收文档。  \*现场登录设备运行检查脚本工具  \*登录设备查看安全配置  2、环境要求  \*提供可以访问网络设备及测评系统的2个IP地址  \*关闭测评IP与系统之间的防火墙。 | 1、准备测评工具及接入方案  2、测评技术人员 |
| 2 | 现场配置检查 | 1、人员要求  网络管理员  \*前期提供网络拓扑图。  \*登录网络设备，配合测评人员检查设备配置。  系统管理员  \*登录网络设备，配合测评人员检查设备配置。  2、环境要求  可登录系统及网络设备 | 1、准备配合检查方案  2、测评技术人员 |
| 3 | 人员访谈 | 1、访谈对象要求  信息部管理人员  \*配合调查表的访谈  系统开发&管理人员  \*配合测评回答应用系统操作相关问题  网络管理人员  \*配合测评回答网络架构，及设备配置操作的相关问题  2、环境要求  提供会议室 | 1、准备访谈安排及访谈大纲  2、测评技术人员 |
| 4 | 文档审查 | 1、人员要求  信息部管理人员  \*提供等保相关的管理制度  系统开发&管理人员  \*提供相应系统建设方案及验收文档  网络管理人员  \*提供网络系统建设方案及验收文档  \*IP规划文档等  2、环境要求  提供办公场所 | 1、准备测评表  2、测评技术人员 |
| 5 | 实地查看 | 1、人员要求  机房管理员  \*配合测评人员检查机房物理环境。  2、环境要求  \*可访问机房、办公等物理区域 | 1、准备测评表  2、测评技术人员 |

**风险规避**

在测评过程中，可能会对被测系统造成影响，相应地会造成各种损失。这些影响包括信息泄露、业务停顿或处理能力受损等。因此，必须充分考虑各种可能的影响及其危害并准备好相应的应对措施，尽可能减小对目标系统正常运行的干扰，从而减小损失。

下表给出了测评过程中可能存在的风险与控制措施。

表10网络安全测评-风险规避

|  |  |  |  |
| --- | --- | --- | --- |
| **内容** | **可能存在的风险** | **等级** | **控制措施** |
| 信息资产调研 | 资产信息泄露 | 高 | 协议、规章、制度、法律、法规 |
| 安全管理测评 | 安全管理信息泄露 | 高 | 合同、协议、规章、制度、法律、法规 |
| 网络设备测评/安全设备测评 | 误操作引起设备崩溃或数据丢失、损坏 | 高 | 规范审计流程；  严格选择测评师；  甲方进行全程监控；  制定可能的恢复计划 |
| 网络/安全设备资源占用 | 低 | 避开业务高峰；  控制扫描策略（线程数量、强度） |
| 漏洞扫描 | 网络流量 | 低 | 避开业务高峰；  控制扫描策略（线程数量、强度） |
| 主机资源占用 | 低 | 避开业务高峰；  控制扫描策略（线程数量、强度） |
| 控制台审计 | 误操作引起系统崩溃或数据丢失、损坏 | 高 | 规范审计流程；  严格选择测评师；  甲方进行全程监控；  制定可能的恢复计划； |
| 网络流量和主机资源占用 | 低 | 避开业务高峰 |
| 应用测评 | 产生非法数据，致使系统不能正常工作 | 中 | 做好系统备份和恢复措施 |
| 异常输入（畸形数据、极限测试）导致系统崩溃 | 高 | 做好系统备份和恢复措施 |

**商务要求**

**1、合同履行期限**：3包网络安全等级保护测评服务：合同签订后至整体海南省医疗保障综合管控系统扩展和多层次医疗救助一体化平台建设项目通过竣工验收。

**2、项目的实施要求**

测评项目实施过程中，投标人应遵循国家标准、行业标准。

项目实施要求

在项目实施中投标方必须做到:

（1）合同签订后，测评单位需立即安排驻场人员全程参与海南省医疗保障综合管控系统扩展和多层次医疗救助一体化平台建设项目建设过程的测评工作，及时协助采购人发现并指导系统承建方完成问题整改工作

（2）提供项目实施组织架构;

（3）提供详细的项目实施方案和计划进度说明书;

（4） 对于采购人的电话咨询和常规服务请求在 30 分钟内予以答复，紧急服务请求在2小时内到达采购人现场;

（5） 严格按照双方确定的计划进度保质保量完成工作;

（6）规范项目实施过程中的文档管理;

（7）项目实施中要引入风险管理、质量管理、成本管理;

（8）签署《保密协议》。中标单位(含项目组所有成员)必须对项目技术文件以及由招标人提供的所有内部资料、技术文档、数据和信息予以保密。中标单位必须与招标人签订保密协议并严格遵守，未经招标人书面许可，中标单位不得以任何形式向第三方透露本项目标书以及本项目的任何内容。

（9）测评实施团队要求和等级测评师证书，复印件需在投标文件中提供，并加盖公章。

（10）按照公安部对测评机构管理的规定和要求，测评项目现场实施的人员必须是本机构的持证测评师，而且测评项目不允许分包或转包，中标人一旦出现和等级测评师证书，复印件需在投标文件中提供，并加盖公章。

（11）按照公安部对测评机构管理的规定和要求，测评项目现场实施的人员必须是本机构的持证测评师，而且测评项目不允许分包或转包，中标人一旦出现上述违规情况采购人有权解除合同。

**3.项目验收标准和方式**

**在初验前向采购人正式提供差距测评报告，差距测评报告包含单元测评、整体测评、风险分析、报告编制。**

（1）中标单位完成技术服务工作的形式：对信息系统安全保护等级进行安全现状分析。依据《网络安全等级保护基本要求》，对物理机房、网络结构、信息系统等进行合规性检查，发现信息系统与安全保护等级要求之间的差距，并出具《网络安全等级保护测评报告》及提出具有针对性的整改意见。

由海南省医疗保障局统一组织，采购人与相关人员组成验收小组完成验收。双方根据最终验收情况，编写《网络安全等级保护测评报告》最终验收报告。中标人应完成项目验收资料的准备。

在服务过程中出现性能指标或功能上不符合标书和合同要求时，由中标人负责解决，采购人有拒绝验收的权利并保留索赔权利。

本项目的实施过程中将产生大量的技术及管理文档，中标人应协助采购人，负责建立、维护、交接项目实施过程中产生的各类文档，确保项目文档的内容体现本项目的实施过程，并确保项目文档的完整性和准确性。

交付物：出具整改意见和测评报告，协助完成系统定级专家评审工作，完成本次测评报告在公安部门的备案工作，并取得有效的备案证明。

（2）成交服务商完成技术服务工作的形式：对信息系统安全保护等级进行安全现状分析。依据《网络安全等级保护基本要求》，对物理机房、网络结构、信息系统等进行合规性检查，发现信息系统与安全保护等级要求之间的差距，并出具《网络安全等级保护测评报告》及提出具有针对性的整改意见。

（3）技术服务工作成果：提交《网络安全等级保护测评报告》作为验收成果。

（4）技术服务工作成果的验收方法：确认成交服务商所进行的技术服务工作均按有关标准及合同要求进行。

（5）验收的时间和地点：按照合同约定，在项目执行完毕后5个工作日内，在甲方指定地点进行验收。

（6）验收组织

成立由采购人、中标方以及其他有关人员组成的验收小组，负责对项目进行全面的验收。

**4.项目工期**

项目实施工期：合同签订后15天内，测评单位需立即安排驻场人员全程参与项目建设过程的测评工作，及时协助采购人发现并指导系统承建方完成问题整改工作并交付测评服务成果。

技术服务质量要求：依据国家和行业指定标准开展测评工作，及时出具符合等级保护管理部门要求的测评报告并协助采购人完成备案。须指导系统承建厂商按照安全相关规定达到测评合格验收标准。

**5.售后服务要求：**

对于测评过程中发现的安全问题，成交方应先出具问题汇总报告，并给采购人预留三十天的整改时间，整改完成后成交方提供一次全面问题复查，并出具最终版测评报告。同时成交方针对本次测评范围内的问题提供一年期的远程技术咨询服务。

**6.培训要求**

对于等保测评发现的问题，需要组织对医疗保障信息平台系统有关各参与方和相关应用系统开发商，进行等保整改建设使用等方面专业知识培训。利用等级保护测评过程，由中标方对招标方工作人员进行相关的培训，包含但不限于工具的使用、渗透测试技术等。

具体要求如下：

（1）投标人应在投标文件中给出详细的培训方案；

（2）培训人应拥有从业相关经验，提供培训人的详细背景资料；

（3）投标人应提供中文培训资料；

（4）如培训未达到预期效果，培训时间进行延长；

（5）培训地点为采购人指定地点；

（6）培训所需费用由投标人承担；

（7）培训时间由海南省医疗保障局按照项目进展情况指定，原则不超过20天。

（8）培训次数：测评过程中现场集中培训两次和线上培训。

**7.其他工作**

（1）协助招标方完成多层次医疗救助一体化服务平台和数据专区（多层次医疗救助基础信息管理系统、多层次医疗救助数据共享中心、多层次医疗救助业务标准规范管理系统、应用支撑基础系统、医疗救助子系统、多层次医疗救助门户系统、数据共享子系统、数据专区）；综合管控系统拓展和医保场景监控（电子处方与药品双通道监管、DRG/DIP监管系统、门诊统筹监管、两库管理与论证系统、医保场景监管系统）2个系统基于三级等级保护的要求作必要的安全检测与评估。这些系统经整改完成后，投标方须承认该系统已通过等级保护测评企业主持的等级保护测评。”

（2）投标方须提供完整方案。

**8.其他说明：**

（1）若测评结果符合要求，需测评单位出具说明，测评结果符合要求，需测评单位公司法人或授权代理人签字、盖章。

（2）对测评过程中发现的问题，测评单位须提供有效的解决方案并协助指导相应系统承建方完成整改，符合海南省省本级政务信息化项目验收管理规范中对等级保护安全性评估要求，达到新建项目验收标准。

（3）海南省医疗保障综合管控系统扩展和多层次医疗救助一体化平台建设项目需总体终验合格后向项目各包支付项目款项。

（4）合同签订后，测评单位需立即安排驻场人员全程参与项目建设过程的测评工作，及时协助采购人发现并督促系统承建方完成问题整改工作.

**9.项目管理要求**

（1）采购人与成交方双方分别成立项目工作组、项目实施组。在项目实施过程中，成交方应保证项目工作组成员的稳定，如变更项目组成员必须事先征得采购人的书面同意，且替换人员的相关资质不应低于原项目人员的资质水平；

（2）成交方为本项目投入技术人员不少于 5 人，实施期间提供驻场不少于 3 人的 项目实施团队（包含 1 名项目经理），该团队的技术人员应具有等保测评师证书；

（3）成交方应保证，在项目实施中不能影响系统的正常运行和使用，项目实施应依据国家标准、行业标准等相关要求和标准进行；在服务期内，工作要做到事事有记录、事事有反馈、重大问题要及时汇报。严格遵守工作作息时间，严格按照服务工作流程操作。

## （4）投标人派驻现场人员与投标文件中的人员不一致，除非不可抗因素，只允许重新指派一次，且更换的人员必须为原同等资质证书人员，否则视为中标单位放弃合同。

二、产品的安装调试、试运行和验收标准要求

1. 本项目为交付承包项目，中标供应商承包及负责招标文件对中标供应商要求的一切事宜及责任。包括项目产品供货、配套设备提供、运输、保管、安装、调试、验收、培训及相关服务等以及投标人认为必要的其他货物、材料、工程、服务；投标人应自行增加系统正常、合法、安全运行及使用所必需但招标文件没有包含的所有设备、版权、专利等一切费用，如果投标人在中标并签署合同后，在供货、安装、调试、培训等工作中出现货物的任何遗漏，均由中标供应商免费提供，买方将不再支付任何费用。

三、技术资料

投标人应保证所提交给招标人和招标代理机构的资料和数据是真实的，因提交的资料和数据不真实所引起的责任由投标人自行承担。

四、工具

投标人提供产品所带专用工具清单，并标明其种类、用途和生产厂，并在货物到货时同时提供给业主，此价格应包含在投标价中。

五、质量保质期

**本项目的质保期最低为两年，质保期从整体验收合格之日起计算**，免费上门服务**。**（采购清单中免费保修期有特殊要求的按照采购清单中的为准）。

六、签订合同：中标供应商在收到《中标通知书》5个工作日与业主签订合同。