第三章　　采购需求

A 包："村医通"终端运维（含流量卡）

一、"村医通"终端运维方案

"村医通"系统于 2020 年 8 月份正式上线，2021 年 10 月 29 日终验，项目总计采购设备 3000 台"村医通" POS 医保终端，在海南全省范围内的部署规模庞大，涵盖了 2754 台设备，服务于 434 家卫生院、2252 家卫生室以及 68 家社区，各市县备用机 246 台。这一设备部署现状充分展示了海南省在基层医疗服务数字化和信息化方面取得的重要进展。这一广泛的覆盖确保了更多的患者能够享受到便捷的医疗服务，也提高了基层医疗机构的数字化水平。截至目前，全省总体医保结算 143704 人/次，结算金额 2901689 元。且已为用户维修 167 台设备，其中维修内容主要为：更换屏幕、更换硬件主板、物联网卡槽维修、二代身份证读卡器更换，热敏打印机维修等多个方面硬件维护服务，保障设备的高效运行，为用户提供持久而稳定的服务。

项目质保服务工作已于 2023 年 12 月份到期，为了确保"村医通"系统的正常稳定运行，在全省医保统筹管理上，按规定维护管理流程，需要对"村医通"继续进行运维。以购买社会服务方式，驻场人员对"村医通"软硬件设备进行运维管控。

1、服务内容：

运维服务内容包括日常维护、应急性维护、适应性维护、完善性维护、整体优化服务、定期巡检服务、事故分析服务等服务，以保证系统的正常运行。具体的技术服务内容如下：

1.1 系统日常维护

日常维护主要是针对系统操作人员在日常业务办理中，因为操作错误所引起的系统错误进行维护；以及对系统在开发过程中因各种原因遗留的 bug 进行修正；日常维护的内容包括：

- 日常操作操作维护；
- 日常数据错误维护；
- 应用系统 3 级缺陷修复；
- 用户日常操作培训。

1.2 应急性维护

当系统出现系统整体性能急速下降，严重影响系统的正常运行，导致部分或全部系统不能正常办理时，进行应急性服务，帮助用户在最短时间内，恢复系统正常状态。

保障系统的稳定运行是一个综合工程，引起系统性能急速下降的原因甚多，例如：主机系统的问题、网络系统的问题、存储系统的问题、系统平台的问题、应用系统的问题，误操作引起的问题等等。在进行应急性维护时，需要用户进行充分的协调工作，从多方面综合查找原因，以利于快速的发现问题，解决问题。

1.3 适应性维护

适应性维护是针对软件系统为适应外部环境的变化进行的系统修改活动，例如：作为行业的应用系统，政策调整不可避免，当系统已不能通过政策参数的调来适应政策调整要求的时候，进行应用系统的适应性维护。

为保证应用系统版本的一致性，此类完善性维护，不在用户现场完成；由维护人员接受用户请求后，将应用系统的适应性需求提交给运维公司产品维护组进行统一的产品完善后，再部署到用户服务器上。运维公司产品维护组配备了一批技术力量强，熟悉本产品、经验丰富的工程师，对本产品进行统一的维护、测试，即保证了产品版本的一致性，也保证了产品设计的整体性，和应用系统的高性能，为系统的长期稳定运行打下良好基础。

1.4 定期巡检服务

制定应用系统巡检服务计划，根据计划执行巡检计划；记录巡检结果，根据巡检情况完善系统优化方案。建立系统运维档案，详细记录系统运维情况，对每次运维工作进行跟踪；所制定的运维档案指导巡检计划的优化。

1.5 事故分析服务

在每一次故障排除或常规检查之后，进行做详细的记载，提交系统运维档案；对每一次故障均做出详细故障原因分析报告，及时给出适当建议。

1.6 设备定期巡检硬件组件

定期派遣技术人员到现场进行回访，及时了解设备的运转情况，及时解决存在的问题。

（1）处理器和内存

检查处理器使用率： 定期检查处理器的使用率，确保在正常工作负载下，处理器性能足够满足需求

内存检查： 确保内存容量充足，避免因内存不足导致系统运行缓慢。

（2）存储设备

健康状态检查： 定期检查存储设备的健康状态，包括存储容量、可读写性等，确保足够的存储空间和数据安全。

（3）连接线路和端口

物理连接检查： 检查所有连接线路和端口，确保连接牢固，防止因松动导致的连接中断。

（4）热敏打印机

连接状态测试： 检测热敏打印机的连接状态，打印字迹清晰度，确保它们能够正常工作。

1.7 设备定期维护服务内容

定期维护服务主要包含两个方面：

（1）定期系统巡检，由运维单位组织巡检人员协同维护工程师进行周期性的定期系统巡检。

（2）规定维护工程师组织定期系统保养。针该对该项目，维护单位在一年内不低于四次的资深工程师现场评估，其主要内容包括：系统整体检测、硬件评估、维护工程师的考核。

系统整体检测具体内容有：

- 设备故障隐患排查
- 设备各项功能性检查
- 设备重要性能指标检查
- 系统运行稳定性检测
- 系统运行安全可靠性检测
- 系统重要数据备份
- 系统软件维护和升级
- 设备工作环境检查
- 设备的运行状态检测

1.8 设备故障维护

对于出现故障的设备或零部件、接插件，维护单位负责排查及分析原因，根据故障设备是否在维护期内提供维修方案：

（1）设备或零部件在维护期内的，使用备用机临时替换下来，将有故障的设备送至售后维修中心处理，后续厂家维修好之后再替换回原来的位置，此维修为免费。

（2）设备出现无法开机、屏幕故障等配件无法临时替换，将故障的设备送至厂商售后维修处进行维修，并且承担维修所需费用及物流费用，此维修为免费。

1.9 交付成果：《海南省医疗保障局“村医通”便民服务工程运维服务报告》

二、“村医通”业务系统优化方案

1.1 业务概述

“村医通”主要针对城乡居民医保参保人提供医保实时联网结算，医保缴费和养老生存认证业务功能。开发优化需求包括如下功能点：

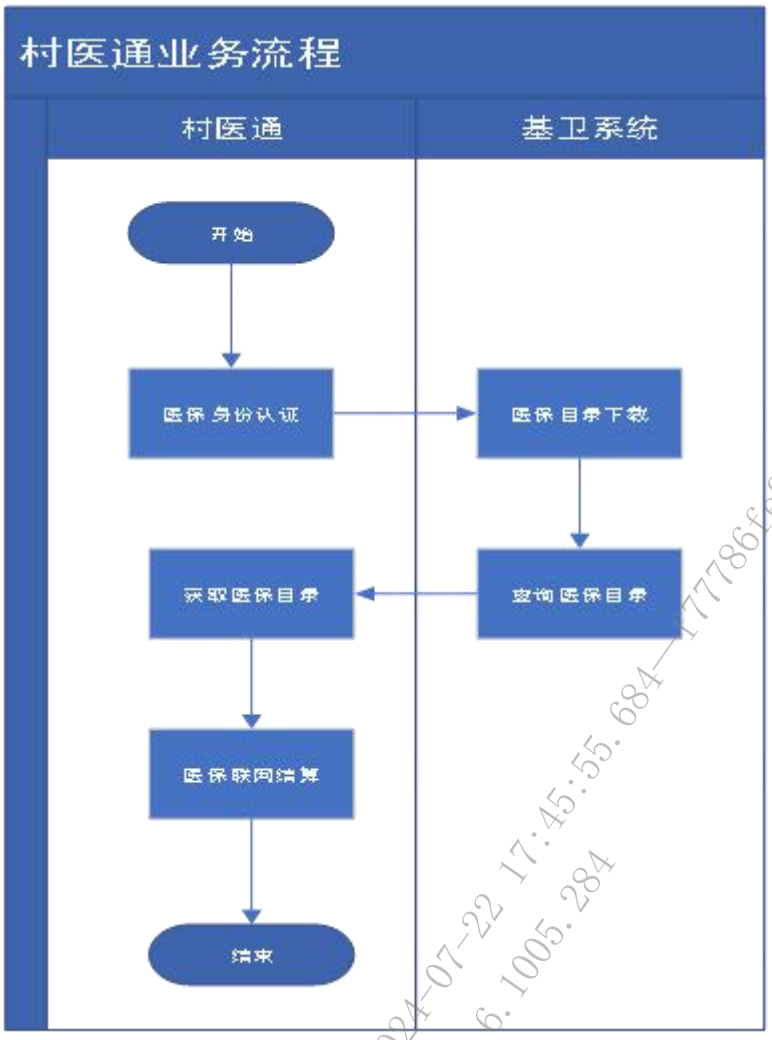
医保结算：医保实时联网结算。

结算退费：医保结算联网撤销。

医保身份认证：进行医保结算前需通过人脸识别，刷身份证或社保卡等途径完成身份认证。

医保目录下载：获取最新版本医保目录。

1.2 业务流程图



1.3 特殊要求

“村医通”主要针对城乡居民医保参保人进行医保门诊实时联网结算。

三、“村医通”设备流量卡租用

海南省“村医通”便民服务工程项目设备流量卡租用包含 3000 张 500M 无线流量卡费用。

序号	名称	要求	单位	数量
1	流量（MB/卡/月）500M	“村医通”POS 机配套 4G 卡，采用流量池管理。	张*月	36000
2	“村医通”便民服务工程终端接入管控服务费	“村医通”POS 机配套 4G 卡联网组网，网络安全保障、链路加密、终端接入管控、联网质量保障等配套服务。	年	1

设备流量卡租用通信服务要求：

1、传输时延

当信息（包括视音频信息、控制信息及报警信息等）经由网络传输时，端到端的信息延迟时间（包括发送端信息采集、编码、网络传输、信息接收端解码、显示等过程所经历的时间）应满足下列要求：

海南省医疗保障局至市县医保局、区医保局、医院、卫健委等相关单位之间端到端的信息延迟时间应不大于 2s。

2、传输质量

网络的传输质量（如传输时延、包丢失率、包误差率、虚假包率等）应符合如下要求：

（1）网络时延上限值为 400ms；

（2）时延抖动上限值为 50ms；

（3）丢包率上限值为 1×10-3；

（4）包误差率上限值为 1×10-4。

3、服务其他要求

（1）运营商需提供流量监管、网络安全、接入质量分析、接入管控等服务；

（2）运营商需提供定向流量服务相关覆盖率分析、质量提升方案、接入管控等服务。

四、商务要求

1、服务期限：合同生效之日起一年。

2、交付地点：用户指定地点。

3、交付方式：免费送至用户指定地点。

4、采购资金的支付方式、时间、条件：本项目经费采用两次付款支付方式。

4.1 合同签订生效后，甲方凭乙方提供的正式有效等额发票，在 10 个工作日内向乙方支付合同总价的 40%。

4.2 合同服务期满，以设备正常使用率及网络通畅率为依据据实结算及支付尾款：全省范围内，设备正常使用率且网络通畅率均大于等于 95%，甲方向乙方支付运维服务费用总价的 60%；设备正常使用率且网络通畅率均大于等于 85%并小于 95%，甲方向乙方支付运维服务费用总价的 50%；设备正常使用率且网络通畅率均小于 85%，甲方向乙方支付运维服务费用总价的 40%。服务内容经甲方验收

后，甲方凭乙方提供的正式有效等额发票，在 10 个工作日内向乙方支付相对应的运维服务费用。

5、验收要求：按标书服务要求和国家行业标准进行验收，“村医通”设备流量卡需确保开通并可正常使用，否则不予验收（提供承诺函加盖公章）。

6、其他要求：

6.1 乙方应根据甲方实际需要进行设备功能优化及调整。(提供承诺函加盖公章)

B 包：安全咨询及保障服务

一、安全咨询及保障服务内容

序号	运维对象	备注
1	安全态势预警与通报服务	合并边界实时监测服务、安全事件实时监测服务。系统渗透测试服务及安全态势预警与通报服务要求 1 名高级安全服务人员。2024 年度服务期共计为 4 个月，本服务按照 4 人月计算。
2	安全大数据综合服务	安全大数据综合服务要求 1 名高级安全服务人员。2024 年度服务期共计为 4 个月，本服务按照 4 人月计算。
3	安全驻场保障服务	安全驻场保障服务要求 2 名高级安全服务人员进行估算，按 8 人月计算。2024 年度服务期共计为 4 个月，本服务按照 4 人月*2 计算。
4	安全设备运营服务	安全设备运营要求 1 名高级安全服务人员。
5	应急演练与攻防演练服务	服务期内开展演练工作，要求 1 名高级安全服务人员，按 4 人月计算。2024 年度服务期共计为 4 个月，本服务按照 4 人月计算。
6	重保服务	重保服务要求 1 名高级安全服务人员，按 4 人月计算。2024 年度服务期共计为 4 个月，本服务按照 4 人月计算。

（一）安全咨询及保障服务方案

海南省医疗保障局于 2023 年 6 月采购了安全咨询与保障服务，服务期限为一年。该项服务的主要内容包括对海南省医疗保障信息平台整体网络与安全进行监测监管，以提升医保平台的整体安全性。该项目服务周期将于 2024 年 8 月截止。为确保医保局及医保平台的服务质量，本次将采购网络安全服务运维项目，具体服务方案内容如下：

根据《中华人民共和国网络安全法》第十七条中国家推进网络安全社会化服务体系建设，鼓励有关企业、机构开展网络安全认证、检测和风险评估等安全服

务的要求，从符合性的角度分析出医疗保障信息平台二期信息系统和“村医通”应用系统的技术防护需求，立足海南省医疗保障局的职能定位，围绕“没有网络安全就没有国家安全，没有信息化就没有现代化”的态势，并结合实际情况，在已有信息化建设和网络安全设备的基础上，通过采购网络安全服务，更好地为海南省医疗保障局信息网络安全保障工作、重要信息系统安全防护工作提供全面、及时、准确的情况通报、事件分析报告，特别是在重大活动安保工作中有能力对海南省医疗保障局突发情况进行准确的研判和对重点部位、重要情况进行预警，有必要采购安全监测服务和现场安全运维服务等，提升对网络安全态势的总体掌控能力，同时为信息安全日常工作提供支撑。清单如下：

序号	服务项目	
1	安全态势预警与通报服务	1、通过汇聚互联网全流量测数据及医保系统平台流量数据、日志数据、安全防护设备数据进行网络安全威胁大数据关联分析、交叉验证及人工核验，综合研判网络安全风险隐患并及时进行预警通报。 2、安全态势预警与通报服务能够对业务系统及网络边界提供 7x24 小时持续监测服务，监测对象包括云平台、业务系统，针对网络入侵、异常流量、僵木蠕、系统漏洞、全流量监测及网站监测六个方面进行监测，监测过程发现安全事件实时发出告警，并通过系统页面、邮件或者短信方式通知相应管理员。 3、针对发现的僵尸、木马、蠕虫、DDoS 攻击、域名等安全事件结合威胁情报等数据进行关联分析，验证事件的准确性，并对确定的事件提供研判过程、详情解释、处置建议等。 4、针对平台发现的网站安全漏洞进行漏洞审核或验证，包括但不限于 SQL 注入漏洞、XSS 漏洞、参数污染、JAVA 漏洞、文件包含漏洞等漏洞验证工作，确保漏洞的准确性，对漏洞进行详情解释和处置建议。 5、针对预警通报的安全事件提供整改加固咨询。 6、为满足业务云环境部署条件，服务工具必须满足软硬一体化形态和纯软件形态部署模式，软件形态支持部署在物理机/虚拟机/云环境；服务工具应内置包括规则模型、关联模型、统计模型、情报模

		型、AI 模型等不少于 5 类安全分析模型； 服务工具应满足安全分析模型支持自定义创建，可通过字段映射、静态值、模板、表达式等多种方式自由定义分析模型的告警名称、威胁等级、告警类型、攻击链、可选字段、告警描述、处置建议等内容； 7、系统渗透测试服务及安全态势预警与通报服务要求 1 名高级人员驻场。
2	安全大数据综合服务	基于互联网全流量监测数据并汇聚医保系统平台流量数据、日志数据及安全防护设备数据进行网络安全威胁大数据关联分析、交叉验证等态势研判，实现从不同视角感知医疗保障信息平台网络安全态势，包括总体态势、威胁态势、攻击态势、隐患态势、事件态势五大视角。 1、网络安全总体态势分析，包括当前数据来源、监管对象统计、监测成果统计、漏洞与隐患详情、隐患、攻击、事件、通报的趋势、系统隐患数量 TOPN、隐患区域 TOPN、事件分布统计、通报处置列表等内容。 2、威胁态势分析。内容包含威胁分类及统计、威胁源分布及统计等。 3、支持隐患态势分析。内容包含隐患分类及统计、隐患区域和行业分布情况等。 4、网络攻击分析，内容包含网络攻击分类及统计、监控总览及分类、最新攻击消息、攻击趋势、受攻击行业分布、攻击类型分布、攻击区域/受攻击区域排名、攻击 IP/受攻击 IP 排名等。 5、安全事件分析，内容包含重点监测系统数、安全事件数、安全事件分类统计、事件趋势、最新事件概览、事件类型分布、事件区域排名等。 6、服务工具应具备全局资产的资产访问图谱可视化模块，支持立体、平面、球面等多种维度的网络实体关系透视。根据资产的风险等级，对资产用不同颜色进行区分，具备访问关系的资产用直线相连，访问关系具体说明，包括但不限于：访问方向、访问类型、累计流量、访问时间等。服务工具应支持每个用户配置个人专属的统一门户，

		可配置项包括门户名称、应用名称、应用图标等。服务工具应统一门户，应支持与第三方产品集成，一键跳转至产品功能界面。服务工具应支持一键访问安全设备的管理界面、监控大屏、设备日志、处置联动记录；该服务工具应与安全态势预警通报联动，或整合为统一管理平台。 7、要求 1 名高级人员驻场。
3	安全驻场保障服务	安全驻场保障服务：为保障常态化服务能力，除安全咨询服务内容范围外，提供现场运营、预警、处置、协调人员。应急演练期间现场咨询服务人员 2 人。
4	安全设备运营服务	1、提供具有丰富的设备调试、策略维护的工程师，根据业务需求开展常态化运行过程中所进行的一系列运营维护工作，包括安全产品运行安全监测、策略配置、产品升级设计及策略备份等工作。 2、安全产品运行监测，信息系统运行过程中，可能面临安全产品运行异常、安全事件的发生等情况，为有效应对这些情况的出现需要开展长期的安全产品运行监测工作，以及时发现并按照流程有效处理； 3、安全产品策略配置，安全防护是通过全面落实安全策略、合理配置安全产品防护规则，对来自各网络区域的网络攻击行为进行防护； 4、安全产品升级，安全设备的有效性除了合理配置安全策略，还应该定期对安全设备的软件版本、特征库进行升级，确保安全设备的安全稳定运行的同时，也确保安全设备规则的最新； 5、安全产品策略备份，为确保安全产品在出现异常故障时能够及时恢复，需要定期对安全产品策略进行备份，防止策略意外丢失等情况造成的严重后果； 6、为保障常态化服务能力，提供 1 名信息安全工程师驻场工作。
5	应急演练与攻	根据《中华人民共和国网络安全法》《国家网络安全事件应急预案》《中华人民共和国突发事件应对法》《突发事件应急预案管理办法》、国家《信息安全技术 网络安全等级保护基本要求》（GB/T

	防演练服务	28448-2019）、《海南省信息化条例》和《关于印发海南省党政机关、事业单位和国有企业互联网网站安全专项整治行动方案的通知》等文件对“网络安全事件应急预案、应急演练、应急响应”的相关规定，结合用户信息系统的实际情况，帮助并指导采购人建立健全网络安全事件应急演练工作机制，并对信息系统相关人员进行应急预案、应急技巧及对典型的网络安全事件进行预防等方面的培训，指导和协助其进行 1 次应急演练活动，从而有序地开展，防范并及时、高效处理网络与网络安全突发事件，保障重要信息系统安全、稳定、持续运行，最大限度地减少网络安全突发事件带来的影响，预防造成重大损失和影响。 1、攻防演练宣贯：组织以内容为红蓝对抗模式、攻击方思路、防守方的培训；对抗准备及实施：工具准备及对抗实施； 2、复盘总结：讨论攻防过程中的细节，总结蓝方攻击手段和成果，红队监测和防护成果，结合实际防护情况提出优化建议，固化红蓝对抗成果； 3、报告编写：总结红蓝对抗过程成果，提供安全建议。
6	重保服务	1、协助用户单位做好特殊时期(如春节、国庆、护网等)的信息安全保障工作和值班:服务器、网络、安全等新设备接入网络时进行安全性、可用性检查。特殊情况下,增派资深安全专家并协调相关外部资源。协助用户单位全面构建重保时期的网络安全积极防制体系、从重保单位信息系统的需求、设计、开发、上线和运行等各个阶段，加强信息系统生命周期安全管理、协助被保障单位建立全面的主动安全运备机制、提升被保障单位数据驱动的威胁对抗能力。 2、重大时刻前，要与用户单位的重点保护目标进行确认，确定出需要重点保护的业务系统目标，然后利用风险评估工具对目标系统开展风险评估工作。尽可能最大程度发现目标系统存在的安全漏洞，并配合用户单位及时对漏科进行修复和加固。 3、重大时刻期间，须要派出经验丰富的安全专家对用户单位目标系统进行安全值守，对系统的安全状况进行实时监测。当发现异常时，

		应采取有效有段或工具进行防护，并出具应急响应报告。 4、重大时刻后，安排专家对网络安全保障工作进行总结和汇报。

人员要求：共 7 人。其中安全态势预警与通报服务要求 1 名高级安全服务人员，安全大数据综合服务要求 1 名高级安全服务人员，安全驻场保障服务要求 2 名高级安全服务人员，安全设备运营服务要求 1 名高级安全服务人员，应急演练与攻防演练服务要求 1 名高级安全服务人员，重保服务要求 1 名高级安全服务人员。

该 7 名安全运维人员供医保局综合调配使用，7 名人员的岗位职责安排、值守排班安排、人员上岗面试、人员绩效考核等，均由医保局统筹安排。

该 7 名安全运维人员除负责信息安全服务外，还负责医保局运维中心值守及至片区医院、村卫生室及药店现场处置协调。

该 7 名安全运维人员互为备份，以确保在人力资源有限的情况下，医保信息系统安全的、不间断地运行。

1.1 安全态势预警与通报服务

根据医保局信息系统项目与大数据管理局约定，省网络安全态势感知平台负责对部署在政务云的数据中心 A、B 提供安全态势感知服务，医保局负责对数据中心 A、B 边界监测，及接入近 3000 家医疗单位及医保定点药店对医保二期平台的威胁感知监测、事件预警及通报工作。

根据《海南省电子政务云计算中心管理办法》，省大数据管理局负责对云中心开展实时安全监测，医保局负责对云数据中心 A、B 边界及下属近 3000 家医疗单位及医保定点药店开展安全态势感知工作。

1.1.1 安全态势预警与通报服务

1.1.1.1 服务要求

安全态势预警与通报服务能够对业务系统及网络边界提供 7x24 小时持续监测服务，监测对象包括云平台、业务系统、各医保网络接入单位，针对网络入侵、异常流量、僵木蠕、系统漏洞、全流量监测及网站监测六个方面进行监测，监测过程发现安全事件实时发出告警，并通过系统页面、邮件或者短信方式通知相应管理员。

1.1.1.2 服务内容

总共提供七个方面服务内容：

（1）网络入侵态势感知服务。针对网络入侵检测设备发现检测到的入侵事件告警，基于攻击链模型，进行事件汇总、分析；支持网络入侵事件监控、同比分析，支持被入侵主机、入侵源的分析。

（2）异常流量态势感知服务。针对异常流量监测系统发现的 DDoS 攻击，进行汇总、分析。支持但不限于流量、攻击类型等方式进行异常流量监控、统计、分析；支持针对不同业务、不同地区、不同类型进行流量统计分析。

（3）系统漏洞态势感知服务。对系统漏洞扫描产生的系统漏洞日志进行汇总、分析。 支持对系统新增、已修复漏洞进行统计分析、支持系统漏洞总数、漏洞类型、漏洞 TOPN 的监控分析。

（4）网站安全态势感知服务。对网站安全监测系统、网站脆弱性监测系统、网站安全管理系统产生的监测日志进行汇总、分析。

（5）僵木蠕态势感知服务。对网络入侵检测系统产生的僵尸、木马、蠕虫及恶意文件告警进行汇总、分析。支持对上述事件的下钻分析，实现影响主机 IP 分析、影响主机数分析、攻击次数分析；支持对上述事件类型的 TOP N 分析。

（6）提供全流量威胁分析服务。针对 UTS 探针上报的告警信息和流量元数据信息，利用规则检测和机器学习引擎能力，及时发现网络安全事件线索，及时检测病毒木马、网络攻击等安全事件情况。实现流量数据的采集和解析工作，可以对流量数据进行逐层解码，将解析后的流量元数据上传至大数据平台，将原始流量 pcap 数据留存在本地硬盘；提供 HTTP 协议、DNS 协议、邮件协议、FTP 协议、TELNET、数据库操作、SSL/TLS 协商记录、登录记录、认证记录、ICMP 协议、TCP 会话、UDP 会话等元数据提取。

（7）态势感知情报分析服务。支持针对资产、地域、IP 进行攻击过程分析，将攻击过程进行可视化呈现，并且支持下钻分析，对各个攻击过程上的安全事件进行详细呈现。能大屏展示出最新攻击源（IP）的分布情况，可通过点击具体 IP 快速获取该 IP 的地理位置、攻击类型、恶意历史记录等信息。输入漏洞的编号或关键字，可进行精确或模糊搜索，能查询出该漏洞的名称、编号、热度、影响范围、解决方案等信息，并能基于厂商、产品类型、风险等级、热度、是否有

POC 等角度对搜索结果做筛选。

1.1.1.3 服务工具要求

（1）为满足业务云环境部署条件，服务工具必须满足软硬一体化形态和纯软件形态部署模式，软件形态支持部署在物理机/虚拟机/云环境；

（2）服务工具应内置包括规则模型、关联模型、统计模型、情报模型、AI 模型等不少于 5 类安全分析模型；

（3）服务工具应满足安全分析模型支持自定义创建，可通过字段映射、静态值、模板、表达式等多种方式自由定义分析模型的告警名称、威胁等级、告警类型、攻击链、可选字段、告警描述、处置建议等内容；

（4）服务工具应支持对安全日志里 200 个以上字段进行任意形式的逻辑与或非形式组合建模，运算方式包括但不限于等于、不等于、大于、小于、大于等于、小于等于、属于、不属于、存在、不存在，并能根据组合方式自动生成运算表达式，字段包括但不限于应用协议、目的 IP、目的主机名、目的端口、目的用户名、数据流方向、情报 IOC 等；

（5）服务工具应内置不少于 4 种机器学习分析场景模型，可检测发现流量异常、网络会话数异常、网址访问失败异常、域名请求数异常等特定场景条件下的安全态势异常；

（6）服务工具应支持自定义部署 AI 机器学习模型，允许用户选用的高级机器学习算法不少于 4 种，通过输入任意指标类数据进行模型训练，发现异常行为并生成安全事件与告警，辅助用户发现潜在的安全风险。

1.1.1.4 服务人员要求

安全态势预警与通报服务驻场服务由 1 名高级安全服务人员提供支撑。

1.1.1.5 服务频率

服务期内提供 7x24 小时不间断服务。

1.1.1.6 服务成果

输出各种安全态势报告，包括电子政务网边界安全态势感知报告、僵木蠕毒安全态势报告、系统主机漏洞报告。交付物包含但不限于以下内容：

《电子政务网态势感知月度安全态势报告》

《僵木蠕病毒安全态势报告》

《系统主机漏洞报告》

《全流量威胁分析》

1.1.2 安全事件实时监测服务

1.1.2.1 服务要求

安全事件实时监测服务对所要求的监测对象进行 7x24 小时监测，监测到安全事件实时报警，不能出现漏报、误报；监测告警频率能够根据实际需要进行调整，告警的方式可以通过邮件、短信等方式发送；整个服务过程自动化，无人工参与。

1.1.2.2 服务内容

对安全事件进行汇总统计，动态梳理当前热点安全场景，如外部攻击者、漏洞利用成功、弱口令、勒索病毒等，帮助海南省医疗保障局聚焦热点安全问题，并对热点场景类型进行重点监测。

安全事件实时监测服务帮助将海量告警汇聚聚合为安全事件，帮助海南省医疗保障局抓住关注重点，减轻海南省医疗保障局分析负担，以安全事件为切入点，以威胁对象为聚合条件，梳理当前告警数据，变海量告警为几十条甚至十几条事件。

以资产为核心视角，直观了解自身网络环境中存在风险资产。结合攻击链进行分析展示，剖析从侦查阶段到获利阶段的资产失陷过程。感知失陷、异常资产，从海量的日志中提取有价值的资产溯源路线。从以下方面进行功能设计。

风险资产视角。通过资产被攻击严重程度展示网络环境中资产安全风险，包括已失陷、高风险、低风险三个维度，并可进一步对各维度资产情况进行钻取分析。安全域风险视角。以资产所属安全域为维度展示网络环境资产安全风险，并可根据安全域进行钻取分析。风险资产列表。为海南省医疗保障局列出当前存在风险的资产列表，方便海南省医疗保障局进行快速处置分析，并支持资产详情钻取分析。

以业务资产为视角，辅助海南省医疗保障局以资产为核心构建面向业务部门和管理层的业务资产管理模型。业务建模重点管理海南省医疗保障局的业务支撑系统，实现业务资产拓扑和资产安全等级评价等，为海南省医疗保障局提供业务实时监控能力，保障海南省医疗保障局业务可持续平稳运行。主要设计包括以下

功能。支持资产自动发现，也可从海南省医疗保障局现有资产平台进行资产信息同步，帮助海南省医疗保障局及时发现环境中资产，避免非法资产入网。支持对资产进行管理，包括修改、删除等管理操作，并根据海南省医疗保障局资产用途和网站结构划分，将资产至少分为内部资产、互联网资产和重点安全资产。

提供业务监控视图，支持根据网络架构自定义资产拓扑，同时也支持拓扑模板导入和拓扑文件导出。支持资产组织聚合，在上层资产模型中，对二级资产模型进行聚合，为运维人员查看提供便利。支持根据具体业务流程自定义构建业务视图，并支持业务模型修改、删除等管理操作。

以 IP 为视角，以互访流量关系为纽带，聚合呈现信息系统内部的所有资产。结合资产安全状态的综合打分评价结果，透视资产自身状态为高危/中危/低危/安全，以及资产间互相访问关系的正常或异常。主要设计包括如下功能。

资产健康状态评价：根据资产安全告警分析所处安全状态，对资产进行状态标记，帮助海南省医疗保障局清晰了解全局资产状态。资产互访关系透视：全局化呈现基于流量梳理发现的所有资产互访关系，访问类型包括正常访问和异常访问，并统计访问次数，访问方向包括访问内网、来源内网、访问互联网、来源互联网，帮助区分外部攻击和横向威胁。此外，支持一键关系拓展，可视化呈现访问关系，帮助海南省医疗保障局清晰查看威胁扩散情况。资产威胁深度追溯：实现对透视页面独立资产的深度追溯，以攻击者视角对资产进行攻击链阶段定位，并对资产相关告警进行聚合呈现，帮助海南省医疗保障局简化海量告警。资产指纹刻画：结合漏洞管理、终端风险管理等刻画资产详细指纹信息，包括资产自身属性信息、流量管控情况、设备安全信息等。

1.1.2.3 服务频率

服务期内提供 7x24 小时不间断服务。

1.1.2.4 服务成果

《安全事件实时监测报告》

1.1.3 边界实时监测服务

1.1.3.1 服务要求

边界安全事件实时监测服务对网络边界进行 7x24 小时监测，监测到安全事件实时报警，不能出现漏报、误报；监测告警频率能够根据实际需要进行调整，

告警的方式可以通过邮件、短信等方式发送；整个服务过程自动化，无人工参与。

1.1.3.2 服务内容

对医保局网络边界进行安全实时监测，对发现的安全事件进行实时告警，定期提供监测报告；提供数据管理、资产管理服务。提供多合一硬件探针、支持服务。多合一硬件探针提供僵木蠕毒分析、入侵事件检测、APT 事件检测服务。提供基于信誉的僵尸网络检测能力，具备可以持续升级的信誉库，IDS 通过信誉库内的恶意网站 IP、C&C 服务器地址的信誉值执行相应的检测动作；提供敏感数据外发的检测功能，能够识别通过自身的敏感数据信息（身份证号、银行卡、手机号等）；提供覆盖广泛的攻击特征库，可针对网络病毒、蠕虫、间谍软件、木马后门、扫描探测、暴力破解等恶意流量进行检测和阻断，攻击特征库数量至少为 6000 种以上。

1.1.3.3 服务频率

服务期内提供 7x24 小时不间断服务。

1.1.3.4 服务成果

《边界安全态势报告》

1.2 安全大数据综合服务

（1）服务要求

基于互联网全流量监测数据并汇聚医保系统平台流量数据、日志数据及安全防护设备数据进行网络安全威胁大数据关联分析、交叉验证等态势研判，实现从不同视角感知医疗保障信息平台网络安全态势，包括总体态势、威胁态势、攻击态势、隐患态势、事件态势五大视角。

①网络安全总体态势分析，包括当前数据来源、监管对象统计、监测成果统计、漏洞与隐患详情、隐患、攻击、事件、通报的趋势、系统隐患数量 TOPN、隐患区域 TOPN、事件分布统计、通报处置列表等内容。

②支持威胁态势分析。内容包含威胁分类及统计、威胁源分布及统计等。

③支持隐患态势分析。内容包含隐患分类及统计、隐患区域和行业分布情况等。

④支持网络攻击分析，内容包含网络攻击分类及统计、监控总览及分类、最新攻击消息、攻击趋势、受攻击行业分布、攻击类型分布、攻击区域/受攻击区

域排名、攻击 IP/受攻击 IP 排名等。

⑤支持安全事件分析，内容包含重点监测系统数、安全事件数、安全事件分类统计、事件趋势、最新事件概览、事件类型分布、事件区域排名等。

（2）人员要求

要求 1 名高级安全服务人员。

（3）服务工具

服务工具应具备全局资产的资产访问图谱可视化模块，支持立体、平面、球面等多种维度的网络实体关系透视。根据资产的风险等级，对资产用不同颜色进行区分，具备访问关系的资产用直线相连，访问关系具体说明，包括但不限于：访问方向、访问类型、累计流量、访问时间等。服务工具应支持每个用户配置个人专属的统一门户，可配置项包括门户名称、应用名称、应用图标等。服务工具应统一门户应支持与第三方产品集成，一键跳转至产品功能界面。服务工具应支持一键访问安全设备的管理界面、监控大屏、设备日志、处置联动记录；该服务工具应与安全态势预警通报联动，或整合为统一管理平台。

（4）服务频率

服务期内提供 7x24 小时不间断服务。

（5）服务成果

《安全大数据综合展示报告》

1.2.1 安全驻场保障服务

1.2.1.1 安全事件处置服务

（1）服务要求

针对市级部门网站、各区（市）县等单位门户网站及重要信息系统提供应急响应及演练服务；对信息安全领域疑似非法攻击事件进行处置，包括突发安全事件远程技术支持；突发安全事件现场技术支持；安全事件溯源及调查取证；保障业务连续性；安全事态控制。事件处置过程对客户公开，并严格遵循信息安全突发事件处置流程（准备——检测——抑制——根除——恢复——总结）。本项服务包含在安全驻场保障服务内。

（2）服务内容

通过人工现场供应方式提供重大安全事件应急响应服务。包括：编制应急响

应预案服务、应急预案演练服务、安全事件分析服务、安全事件溯源服务、安全取证支持服务、安全事件处置服务、重要活动、会议保障服务、事件通告服务、安全预警服务、经验教训总结服务等。

建立应急响应体系，包括：编制应急响应工作预案和流程，并在重大信息安全事件发生时严格按照预案组织实施。分析信息安全事件的类型及产生的原因，进行应急处置，排除隐患，恢复系统正常操作，获取并保存相关证据。信息安全事件处置完毕后 3 个工作日内提交详细的应急工作报告，并提出整改方案和建议。建立应急响应组织，建立完善预防预警机制，建立安全事件分级管理体系，建立应急响应保障措施，进行应急预案的定期测试和演练。

提供远程应急处置协助，包括热线支持、远程支持、现场支持等服务手段。

（3）服务频率

每日响应用户需求，按次数提供安全事件处置服务。

（4）服务成果

交付物包含但不限于以下内容：

提供安全事件分析报告、安全事件紧急通报、安全取证支持服务报告、运维值守报告。

1.2.1.2 安全咨询服务

（1）服务要求

通过提供专业人士所储备的知识经验和通过对各种信息资料的综合加工而进行的综合性研究开发，针对环境内存在的各种网络安全问题，专业人士从管理、技术、体制、机制等各方面提出解决方案，融合发现问题、分析问题、解决问题。通过建立安全管理制度和安全考核体系给出有效的解决方案，从而持续地保证业务的安全运行。本项服务包含在安全驻场保障服务内。

（2）服务内容

参照国家等级保护标准 GB/T22239、GB/T22240 及行业等级保护标准要求，提供重要信息系统信息安全等级保护合规建设过程的专业咨询服务，建立健全的网络安全责任制，完善网络安全规章制度、操作规程、台账、档案、记录等，帮助用户确定网络安全方针和目标。

（3）人员要求

团队成员至少一人同时具备的资质包括 CISP（注册信息安全专业人员）和 CISSP（信息系统安全专业认证）。

（4）服务频率

根据用户需求，根据实际情况提供咨询解决方案。建立安全管理制度，并不断进行完善。

（5）服务成果

- 《咨询解决方案》
- 《安全管理制度》
- 《安全考核制度》

1.2.1.3 安全培训服务

（1）服务要求

管理类培训：对从业人员开展信息安全管理类培训，提供丰富先进的专业知识，有效提高参与培训人员的技术和管理水平，增强参与培训人员的安全意识和技能，提供培训报告。

认证类培训：对从业人员进行人员资质认证培训，提供国家信息安全权威测评机构的授权认证， 并确保参与培训的相关人员在培训考试后取得符合国家标准的资质证书。

实践类培训：对从业人员开展信息安全实践类培训，提供丰富先进的实践、演练服务，在线教育培训与靶场对抗，提供实时在线、同步、异步学习、学习评价、对抗演练与模拟仿真环境，提供培训报告，提升技术人员的实操技能。

本项服务包含在安全驻场保障服务内。

（2）服务内容

管理类培训服务包括的服务内容有：（a）IT 战略规划与项目实施高级课程：IT 战略规划，完整 IT 战略规划过程与案例分析，企事业 IT 架构规划，IT 项目管理。（b）IT 治理体系规划与实施高级课程： IT 治理三大支柱，IT 治理核心，IT 决策治理，IT 激励与 IT 控制， IT 治理体系规划与实施。（c）IT 服务管理课程： 服务战略，服务设计，服务转换，服务运营，持续服务改进。

认证类培训服务包括的服务内容有为注册信息安全专业人员系列认证：（a）国家注册信息安全员、（b）国家注册信息安全管理人员、（c）国家注册信息安

全工程师、（d）国家注册信息安全审计人员、（e）国家注册信息安全开发人员等。

实践类培训服务包括的服务内容有：（a）网络渗透与深度防御课程：搭建拟真攻防对抗环境，动手演练黑客入侵步骤，针对性进行主动全面防御部署分析，在短暂时间内提高实践动手能力和综合防御能力。（b）网络渗透测试能力实践课程：安全攻防基本原理与流程，渗透测试技能，恶意代码，脚本木马，客户端安全（c）网络攻防技术实践培训课程：网络攻防技术概述，网络信息收集技术，网络嗅探与协议分析，TCP/IP 网络协议攻击，网络安全防范技术，Windows 操作系统安全攻防，Linux 操作系统安全攻防，恶意代码安全攻防，软件安全攻防——缓冲区溢出和 Shellcode，Web 应用程序安全攻防。

定制类培训服务根据用户的实际需求提供基于政策解读、行业解读、岗位解读等安全专业技术服务。

（3）服务频率

认证培训根据认证机构的开班时间而定，其他部分根据用户培训类型、相关要求以及规模进行。

（4）服务成果

帮助培训对象提高管理层的管理能力，提升全员的安全意识水平，提升技术人员的实操技能，提高单位整体信息安全保障能力，提供培训报告。

交付物包含但不限于以下内容：

《安全教育服务实施报告》《安全教育服务反馈调查》《培训计划安排》、培训资料、信息安全人员资质权威认证证书。

1.2.1.4 驻场人员分工

配合各类应急演练要求，根据在演练期间，按照医保局要求派驻 2 名高级安全服务人员，主要任务如下：

（1）负责通过运维平台远程监测安全设备、安全软件的运行状态，配合安全态势预警、通报的即时信息，根据医保局授权进行响应，并根据医保局要求形成响应及处置需求，提交安全服务处置人员进行处置，对处置结果编写报告，提交医保局信息办备案；

（2）编制对大数据局安全服务及医保局安全设备、安全软件的运维方案及

计划，并填报运营日志。

（3）编制安全设备、安全软件策略规划及配置手册，并以此为基础对驻场运维人员进行培训、指导演练，以达到所有驻场人员均可以根据常态化保障要求或应急情况调度值守。

（4）按照各级医疗机构、定点药店等，按照海口、三亚、儋州三个片区进行分工。主要负责对三个片区下的接入机构进行联网安全监测、监管，接收安全设备、安全软件、安全服务发送的接入单位告警、预警信息，进行协调、协助处置、编制运维日志、编制处置报告；并协调医保局工作人员或受医保局授权委托，对接入医保网的医院、药店、村医室等进行现场安全核查，以确保接入医保网的终端设备、终端设备中的软件、各客户端软件、插件控件等应装尽装，并进行合规性检测和评估，直到符合接入要求。驻场人员负责医保局运维中心值守及至片区医院、村卫生室及药店现场处置协调。

1.2.2 安全设备运营服务

（1）服务要求

运用先进可靠的信息安全技术，提供 1 名高级安全服务人员开展安全设备运营服务，驻场人员服从甲方工作安排，按照甲方相关工作要求协调各相关安全设备运维单位开展具体工作。

（2）服务内容

为了保证网络安全服务质量，在相关实施方提供安全服务期间，实施方应满足以下安全设备运营服务要求：

①安全设备运行监测，对于安全设备运行过程中可能发生的异常故障等情况开展长期运行监测工作，以及时发现并按照相应流程处置；

②安全设备策略配置，对于安全设备的网络策略及防护规则进行审核，策略或规则变更（新增、停用等）应经审核并报用户单位同意后落实，以有效应对来自不同网络区域的网络攻击行为；

③安全设备升级，为保障安全设备有效性，合理配置安全策略，定期对安全设备的软件版本、特征库、规则库进行升级，确保安全设备稳定运行并具备最新安全防护能力；

④安全设备备份，为保障安全产品在出现异常故障或其他不可控因素时能够

及时恢复，定期对安全设备策略及配置进行备份，防止因故障导致防护缺失等严重后果；

⑤其他工作，驻场期间用户分配的其他保障任务。

（3）服务方式

①远程支持

②现场支持

③E－MAIL 支持服务

④电话支持

（4）服务频率

①现场安全运维值守服务 5*8 小时开展安全值守工作。

②设备调试、策略维护、策略配置、设备升级、备份按照用户需求和实际情况。

（5）服务成果

交付物包括但不限于：《安全设备巡检报告》、《安全设备策略规则配置情况报告》、《安全设备升级情况报告》、《安全设备策略备份报告》。

1.2.3 应急演练与攻防演练服务

1.2.3.1 服务概述

在万物互联时代背景下，“没有网络安全，就没有国家安全”，没有网络安全，就没有网络空间中人的安全。网络安全的本质是攻防两端能力的较量，网络安全应急演练与攻防演练是检验用户整体网络安全真实防护能力的最佳实践之一。 根据网络安全等级保护的安全防护要求，提供安全应急演练与攻防演练服务，旨在帮助用户检验网络安全实战防御能力，提高用户对网络安全事件应急响应的理解与掌握，提高网络安全应急处突能力，从而有序地开展防范并及时、高效处理网络安全突发事件，保障重要系统安全、稳定、持续运行，最大限度地减少网络安全突发事件带来的影响，预防造成重大损失和恶劣影响。

1.2.3.2 服务内容

安全应急演练与攻防演练，是针对信息系统在运行过程中或者操作过程中可能出现的紧急安全问题，进行次模拟应急演练。其目的是加强自有业务安全管理，梳理和完善自有业务系统遇到突发事件后应急处理流程，缩短系统中断时间，全

力保障业务系统安全。本次演练方案为业务平台网页被篡改事件处理专题预案,其目的是为进一步规范网页被篡改事件的处理方法和处理程序,提高对自有业务系统网页被篡改事件的反应速度。

演练事件：

海南省医疗保障局受到恶意人员的网络攻击或病毒木马等,导致业务系统功能异常、非法恶意信息传播或网站被恶意挂马等,对单位造成极大的负面影响和损失等情况。

服务内容:安全意识防护培训、应急预案编制、演练页面准备、演练方案、流程梳理、脚本准备、现场环境准备、现场演练彩排、现场演练环节及总结，服务完成后出具《应急演练与攻防演练报告》。

将通过各层面的攻击渗透及社会工程学攻击渗透的实战攻击手段，对防守单位开展实战攻击，检验相关单位网络安全防护能力，提升网络安全应急处置能力，避免发生重大网络安全事件，保障重要信息系统安全、稳定、持续运行。实战演练结束后，针对本次攻防演练发现的问题，组织相关单位人员，提供配套的安全培训，提出整改意见。服务内容主要包括实战攻击、过程展示与风险控制、实战演练培训及总结三大部分。

序号	服务内容	服务说明	服务对象	主要成果文档	服务频率	服务类型
1	应急演练与攻防演练服务	1.网站恶意篡改事件 2.上传 webshell 木马事件 3.病毒攻击事件 4.拒绝服务攻击事件。	用户单位	《网络安全应急演练与攻防演练报告总结报告》《整改建议》、培训课件和培训文稿等	服务期内根据医保局要求开展演练服务	远程服务、现场服务

1.2.3.3 服务成果

通过应急演练服务，输出《网络安全应急演练与攻防演练报告总结报告总结报告》《整改建议》、培训课件和培训文稿等。

1.2.3.4 服务收益

（1）落实网络安全法，贯彻法律法规要求；

（2）以攻代检，检验实战防御能力；

（3）实战促防，提升意识提升，促成应急处置能力提升。

（二）重保服务

1、重保服务的主要工作就是在重要会议或重大活动期间从网络层面、服务器层面、数据层面为用户构建全方面的重要敏感时期的安全保障服务。保障网络基础设施、重点网站和业务系统安全，提供全方位的安全防守构建咨询以及事前、事中、事后的全面安全建设托管服务，确保企业客户的业务系统能够在重大活动期间安全平稳运行。

2、重保服务人员需具备 CISP（注册信息安全专业人员）资质。

3、重保服务工作内容：

3.1 网站安全综合监控：对网站可用性、黑链、暗链、篡改、挂马等进行监测。

3.2 扫描与评估服务：利用专业安全扫描工具对网站进行脆弱性扫描，人工评估漏洞。

3.3 渗透测试服务：白帽子团队对网站进行人工渗透测试。

3.4 整改与复检：针对漏扫和渗透结果，协助整改，并对整改后的站点进行复检。

3.5 主机加固与检测：利用专业主机安全加固与检测响应工具，防止黑客埋雷。

3.6 高危事件应急演练：协助设计重保期间，高危应急演练场景，并完成演练。

3.7 模拟攻防演练：指导业主方完成攻守演练，发现应急处置的设计缺陷。

3.8 重保期间服务：计划设计保障计划、通报流程、协作机制、处置规范及注意事项等。

3.9 现场值守服务：

（1）重保期间 7*24 小时安全监控与值守，针对网站可用性、黑链、暗链、篡改、挂马及其他安全事件进行分析和处置。

（2）同步外部威胁情况，提前添加 IP 黑名单和设置安全策略。

（3）每小时专属群汇报，每日提供日报，每周提供周报。

（4）远程人工日志分析，每日分析当天 web 全流量、各类告警、安全设备等日志。

3.10 安全通告与预警：重保期间，发生的重大外部安保事件、高危漏洞威胁，

第一时间通报预警，并协助修复。

3.11 入侵审计服务：专家级入侵取证人员现场入驻，分析入侵路径和手段，攻击溯源。

3.12 重保工作总结：对保障工作情况进行总结，提交报告。

3.13 交付成果物：《重要时期安全保障工作方案》、《重要时期安全保障值守报告》、《重要时期安全保障工作总结报告》等。

（三）网络安全运营方案

随着各类安全手段逐步到位，用的不多、效果不好的问题凸显，网络安全工作没有发出与其关系海南省医疗保障局及下属单位重要性、与运维工作不可分割的特殊性、工作量巨大和超越部门支撑全网的重大作用相一致的声音，也极大地削弱了网络维护部门在网络安全工作领域的领导作用，并进一步导致人员配备不足、进入恶性循环，最终影响网络安全保障能力。

为此，本文进一步明确网络安全运营体系内涵，明确各类人员安全工作职责，希望借此强化责任意识、主动意识，结合海南省医疗保障局及下属单位的考核体系，加快建立专业网络安全运营团队、面向全网重要系统、 IDC 以及其他部门互联网应用开展 7*24 小时集中化安全运营。

1、设计基本原则

1.1 网络安全运营体系以管控互联网安全风险和业务系统安全风险为核心。

1.2 网络安全运营体系是网络维护体系的有机组成部分， 需要与日常网络运维工作密切配合，实现安全运营和网络运维一体化。

1.3 各省网络安全运营体系需要与总部远程安全检查、安全培训、安全事件监测通报、互联网安全治理、两部委考核专项工作、定期生产分析和信息通报等进行衔接，实现海南省医疗保障局及下属单位安全运营一体化。

1.4 通过安全技术手段的建设和应用，不断提高自动化水平。

1.5 不断壮大安全人员队伍和提升安全技能，不断提高专业化水平。

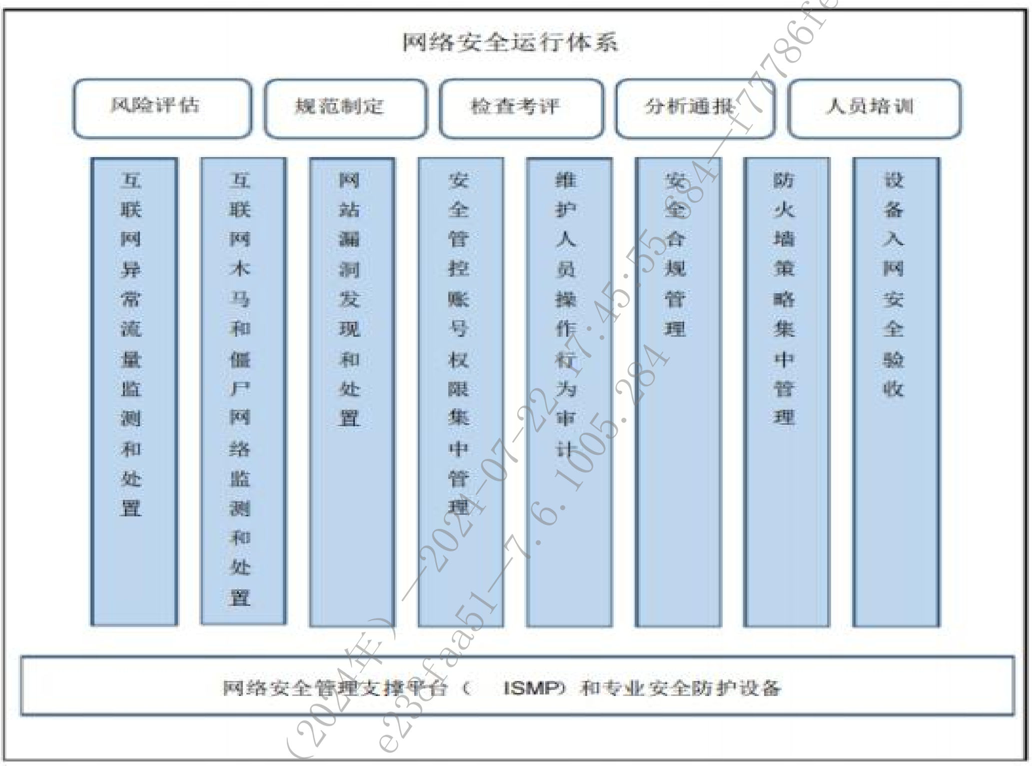
2、主要内容

网络安全运营体系包含以下三方面具体内容：

2.1 由安全专职人员主导各专业配合的横向内容：风险评估、规范制定、检查考评、分析通报、人员培训。

2.2 按照“谁维护，谁负责”的原则，由各专业作为主体进行落实执行的纵向内容：与安全专职人员配合开展互联网异常流量监测和处置、按照安全专职人员监测结果进行互联网木马和僵尸网络处置、网站漏洞发现和处置、基于安全管控平台的网元账号权限集中管理、维护人员操作行为审计、安全合规检查加固、防火墙策略集中管理和核查、设备入网安全验收。

2.3 安全专职人员负责网络安全运行体系的支撑手段，包括网络安全管理支撑平台（ISMP ）以及底层专业安全防护设备的运营工作，各类安全专业防护设备，如互联网异常流量监测和处置、互联网木马和僵尸网络监测运营工作。



3、职责分工

为了更好地推动网络安全运营体系的建立，各省必须逐一细化明确各相关专业的职责分工、具体流程、工作内容、周期要求等，以下内容是对各类人员落实安全职责的基本要求：

3.1 管理层（网络运维部门领导）工作要求：

序号	内容	要求	评价标准
1	明确职责分工	对网络安全运营体系的九项重要工作内容明确安全专职人员和相关系统维护人员的职责界面，协调公司相	有明确的部门发文

		关部门落实安全专职人员配备要求。	
2	听取生产分析	至少每季度听取一次网络安全运营体系生产情况分析报告。	每季度一次生产分析会材料，并提供部门生产分析会纪要。
3	对网络安全运营 体系重大事项进行决策	对网络安全运营体系存在的问题、重大事件进行决策，审定需要通报的内容和范围，并督导落实。	部门生产分析会或者专题工作汇报纪要
4	向省局主管领导进行汇报	每年至少一次汇报网络安全工作内容、整体情况、问题和需要省局领导给予资源支持的决策事项，做到各级人员对网络安全工作特点、内涵、现状、方向的认识完全一致	汇报材料、纪要

3.2 安全专职人员工作要求

序号	内容	要求	评价标准
1	风险评估	定期组织对网络和业务系统的安全 风险评估	1、风险评估的频次不低于等级保护的相应要求，即 3 级及 3 级以上系统每年至少开展 1 次以上等保测评等安全服务，其他系统至少两年开展 1 次评估； 2、评估内容侧重安全渗透； 3、有完善的评估报告和闭环整改证明文档
2	生产分析	定期（月度、季度）对网络安全运营体系的主要工作的执行情况和重大安全事件、问题进行分析	生产分析的频次和各项指标的完整度。

3	安全通报	对网络安全运营体系的执行情况进行通报。	1、通报的频次和通报问题的整改率。 2、至少每 3 个月通报一次。通报内容应全面涵盖文件要求的八个方面的工作内容。 3、通报涉及的系统范围应包括所有与互联网有连接关系的系统，设备范围应包含终端之外的所有主要设备。 4、分析内容应包含多个维度，至少包括：纵向（整改情况）、横向（部门、系统间）、重大或者共性问题专题等。 基于各类自动化安全管理、核查、 漏洞扫描工具，以及数据基本真实准确的安全设备告警（如防病毒、 DDOS 、 WEB 防攻击、僵木蠕）和人工处理内容等。
4	检查考评	制定具体的考评指标，并开展检查 和考评工作。	各类事项的检查频率和覆盖范围不低于集团的要求，即合规、弱口令、防火墙策略核查不低于一季度一次，安全域划分情况核查不低于每半年一次，管控平台接入情况核查不低于每半年一次。
5	闭环管理	对集团公司发现问题、省公司检查发现问题、工单要求、预警公告等	及时整改率

		的落实情况，在明确的处置时间内进行及时复查，全面掌握，直至全 部解决	
6	手段建设	组织规划、需求整理、方案制定、配合建设、协调施工等一系列工作	集团要求的手段建设项目进展顺畅，准确了解进度、问题、未完成任务等
7	手段运营	安全手段策略（如管控平台用户主账号与手机号的对应关系、访问网元使用的账号密码的有效性等）运营，关键数据的定期备份、利用安全手段进行安全核查、扫描等工作，宣传、推动系统维护人员等使用与系统维护职责中安全内容有关的手段。 注：系统主机维护、数据备份可以纳入 IT 维护专业统一管理	集团公司使用省公司管控平台正常 省公司安全手段使用情况

3.3 系统维护人员工作要求

序号	内容	要求	评价标准
1	互联网异常流量监测和处置	确定本系统的流量基线和清洗策略	DDOS 事件发现能力和处理能力
2	互联网木马和僵尸网络监测	负责处置本系统相关的互联网木马和僵尸网络监测事件	互联网木马和僵尸网络事件处置

	和处置		及时率
3	网站漏洞发现和处置	负责对本系统含有的网站进行扫描自查，对自查或者通报的问题进行整改。	网站漏洞处置及时率
4	补丁管理	按照预警公告加载安全补丁，及时升级存在高危漏洞的操作系统、中间件、上层应用和数据库	补丁加载、软件升级及时率
5	账号集中管理	负责对访问本系统的人员账号进行授权、负责本系统资源同步接入和绕行控制配置工作。	口令自动修改率；资源接入率
6	操作行为审计	负责确认对本系统的敏感可疑操作进行审计。对审计判定和实际存在出入的情况，要提出相应证明材料。	违规操作比率；审计事件响应及时率。
7	合规检查	负责对本系统的安全配置和口令复杂度进行自查，并整改不合规项。	每设备弱口令数；设备配置合规率
8	防火墙策略核查	负责配置本系统的防火墙策略，并对防火墙策略定期审核，并过期策略	防火墙违规策略比率。
9	网络安全管控平台的使用	在管控平台正常运行期间，要使用管控平台完成日常操作维护。	管控平台使用率。

二、商务要求

1、服务期限：2024 年 8 月 31 日至 2024 年 12 月 31 日。

2、交付地点：用户指定地点。

3、交付方式：免费送至用户指定地点。

4、项目的实施要求

5、测评项目实施过程中，投标人应遵循国家标准、行业标准。在项目实施中投标方必须做到:

（1）提供项目实施组织架构；

（2）提供详细的项目实施方案和计划进度说明书；

（3）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；

（4）严格按照双方确定的计划进度保质保量完成工作；

（5）规范项目实施过程中的文档管理；

（6）项目实施中要引入风险管理、质量管理、成本管理；

（7）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。

6、采购资金的支付方式、时间、条件：本项目经费采用两次付款支付方式。

6.1 合同签订生效后，甲方凭乙方提供的正式有效等额发票，在 10 个工作日内向乙方支付合同总价的 60%。

6.2 乙方完成项目服务内容，并提交《安全咨询及保障服务项目自评报告》及阶段性工作成果报告且通过甲方组织的验收后，甲方凭乙方提供的正式有效等额发票，在 10 个工作日内向乙方支付合同总价的 40%。

7、验收要求：按标书服务要求和国家行业标准进行验收。

C 包：通信链路租赁服务

一、项目名称

海南省医疗保障局信息化运行维护项目（2024 年）

标包名称：通信链路租赁服务

二、通信链路租赁服务内容

1、通信链路租用服务，包含 582 条通信线路服务费（其中 571 条为付费通信线路。11 条为运营商配套通信线路，为不收费线路）和 2360 张 VPDN 无线流量卡。提供配套的医保专网运营保障（含医保云一体化运营）服务 8 个月，驻场人员 4 人，各地市县须配备接入服务项目经理。

2、通信链路租用(服务期）：2024 年 5 月 1 日至 2024 年 12 月 31 日。

三、通信链路租用方案

1、固网与 VPDN 组网租赁方案

1.1 医疗保障信息平台二期：

序号	线路类型	带宽	用途	单位	数量	备注
1	数字电路	100M	横向单位	条	6	
2	数字电路	6M	一级医院	条	479	
3	数字电路	20M	市县医保局	条	18	
4	数字电路	6M	区医保局	条	9	
5	数字电路	20M	经办机构	条	20	
6	数字电路	100M	A、B 数据中心—省医保局（两条运维、一条业务）	条	5	**由运营商免费提供**
7	数字电路	1000M	备用汇聚专线（各市县运营商专线汇聚，与电子政务外网互为主备）	条	18	

8	数字电路	1000M	政务外网－数据中心（服务商需要具备的链路资源，以满足项目扩展需求）	条	4	
9	裸光纤	裸纤	科工信局	条	17	
10	数字电路	1000M	VPDN 光纤（二期）	条	5	**由运营商免费提供**
11	数字电路	1000M	VPDN 光纤（“村医通”）	条	1	**由运营商免费提供**
12	终端流量卡	10G/月/卡（含接入终端）	桌面终端流量卡，采用流量池管理。	月/卡	27720	
13	办公流量卡	10G/月/卡	医保人员远程办公流量卡，采用流量池管理。	月/卡	600	

1.2 通信线路服务要求：

1.2.1 传输时延

当信息（包括视音频信息、控制信息及报警信息等）经由网络传输时，端到端的信息延迟时间（包括发送端信息采集、编码、网络传输、信息接收端解码、显示等过程所经历的时间）应满足下列要求：

海南省医疗保障局至市县医保局、区医保局、医院、卫健委等相关单位之间端到端的信息延迟时间应不大于 2s。

1.2.2 传输质量

网络的传输质量（如传输时延、包丢失率、包误差率、虚假包率等）应符合如下要求：

（1）网络时延上限值为 400ms；

（2）时延抖动上限值为 50ms；

（3）丢包率上限值为 1×10-3；

（4）包误差率上限值为 1×10-4。

1.2.3 服务其他要求

（1）运营商需提供流量监管、网络安全、接入质量分析、接入管控等服务；

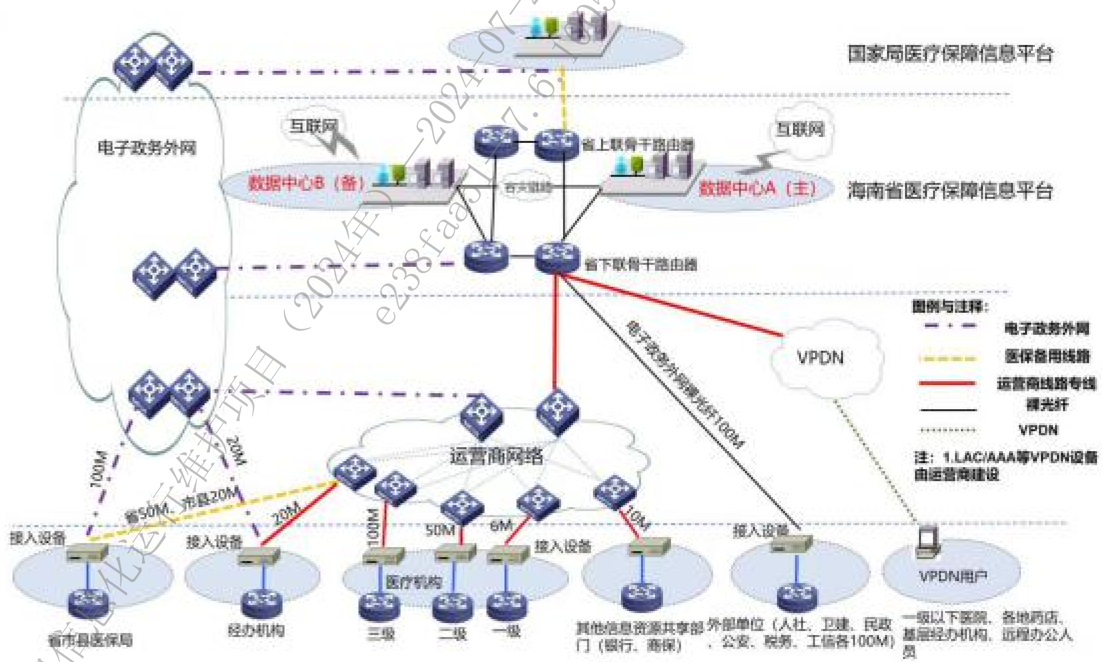
（2）运营商需提供定向流量服务相关覆盖率分析、质量提升方案、接入管控等服务。

2、组网方案

海南医保二期、村医通网络基于电子政务云专属域建设，依托电子政务外网、医保专线、医保 VPDN 网络接入，构建数据共享、交互协同的一体化网络体系，并通过 VPDN 技术为远程办公人员提供访问服务。其中，医保二期医保专线网络光纤网与电子政务外网打通，作为电子政务外网的备线；电子政务外网、医保专线网络光纤网之间起主备路由，保障网络安全。

2.1 医保网组网方案

2.1.1 海南医保二期、村医通网络的总体拓扑结构如下图所示：



2.1.2 医保网整体组网方式如下：

18 个市县一级以上的医疗机构通过各市县运营商专线汇聚，18 个汇聚点采用 1000M 专线与电子政务外网互为主备回传到省医保局数据中心。

一级以下的乡镇卫生所、村卫生室、基层经办机构、远程办公人员等通过VPDN网络接入。

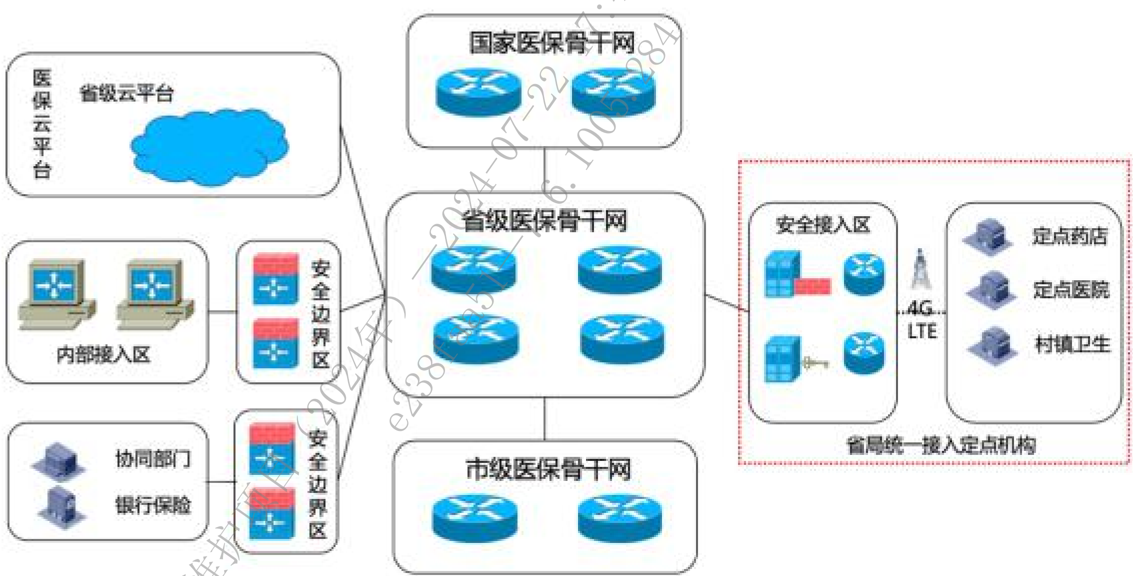
在乡镇、村卫生室信号覆盖不足的地方，考虑就近使用PON专线资源接入进行补盲。

组网所需核心交换机、汇聚交换机、边界防火墙均由链路租赁服务商采购，作为服务费包含在租赁费用中。

医保网接入政务外网、医保网互联网访问的网络安全均由链路租赁服务商提供，作为服务费包含在租赁费用中。

2.2 省级部署模式

依据《全国医疗保障系统核心业务区骨干网络建设指南》相关要求，定点机构接入可采用省级集中部署模式。省级部署模式：省级建设信息平台，市、县级建设网络接入区。各市、县定点医药机构通过安全接入区接入到省级信息平台。拓扑结构如下图所示：



省级部署要求：

省级医保局侧须部署省级CA认证网关、国密IPSEC VPN网关及接入LNS设备。运营商侧须部署AAA鉴权设备、LAC设备等；

定点机构横向接入，须通过医保核心业务区CA强身份认证，认证通过准入。同时，接入设备须在同级医保局安全接入管理平台进行统一认证纳管，才能允许

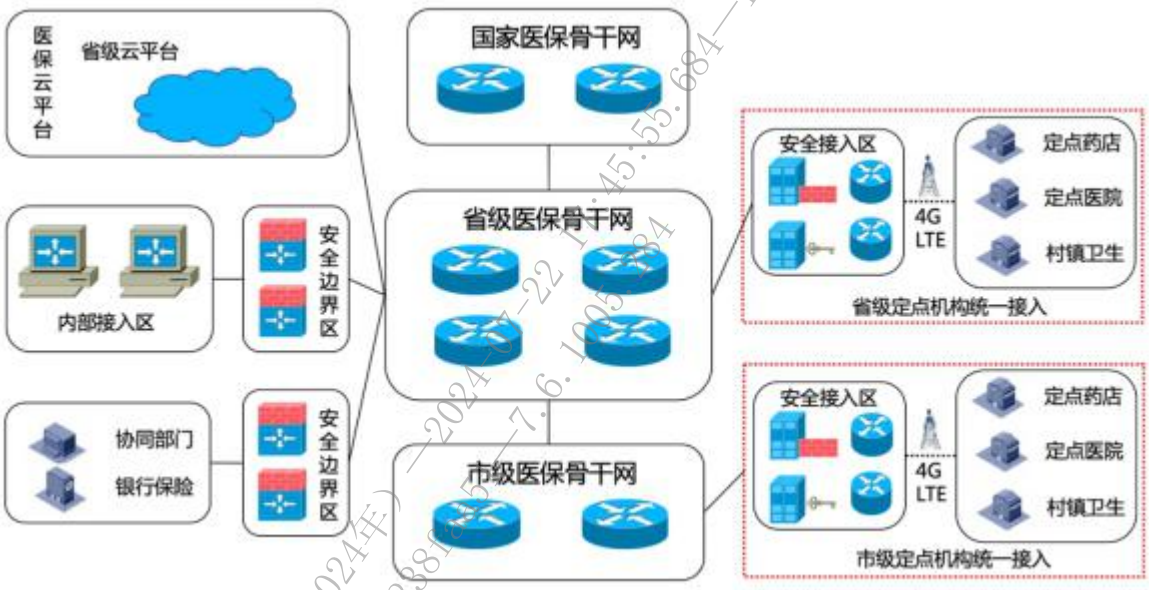
访问医保核心业务区网络。

定点机构接入终端，须部署国家局 CA 身份认证系统颁发数字证书，接入时须进行基于数字证书的强身份鉴别。

省级部署要求的设备，若医保局已建项目中没有采购，则由链路租赁提供商提供，作为服务费包含在租赁费用中。

2.3 省市两级部署模式

依据《全国医疗保障系统核心业务区骨干网络建设指南》相关要求，定点机构接入可采用省市两级部署模式。省级建设信息平台，市、县级建设网络接入区。各市、县定点医药机构等通过安全接入区接入到省级信息平台。拓扑结构如下图所示：



省市两级部署要求：

省级医保局侧须部署省级 CA 认证网关、国密 IPSEC VPN 网关和接入 LNS 设备。运营商侧须部署 AAA 鉴权设备、LAC 设备等；定点医药机构横向接入，须通过医保安全接入区 CA 强身份认证方式，认证通过准入；同时，接入设备须在同级医保局安全接入管理平台进行统一认证纳管后，才能允许访问医保核心业务区网络。

市级侧医保局须部署市级 CA 认证网关、国密 IPSEC VPN 网关和接入 LNS 设备。运营商侧须部署 AAA 鉴权设备、LAC 设备等；定点医药机构横向接入，须通过医保安全接入区 CA 强身份认证方式，认证通过准入；同时，接入设备须在同

级医保局安全接入管理平台进行统一认证纳管后，才能允许访问医保核心业务区网络。

定点机构接入终端，须部署国家局 CA 身份认证系统颁发数字证书，接入时须进行基于数字证书的强身份鉴别。

2.4 组网建设要求

定点机构通过运营商的 4G 专线接入，满足医保业务数据安全传输的基本需要。

VPDN 技术具备以下特点：

（1）灵活方便

满足快速组网要求，具备 3G/4G 网络覆盖就可接入，解决覆盖乡村的难题。

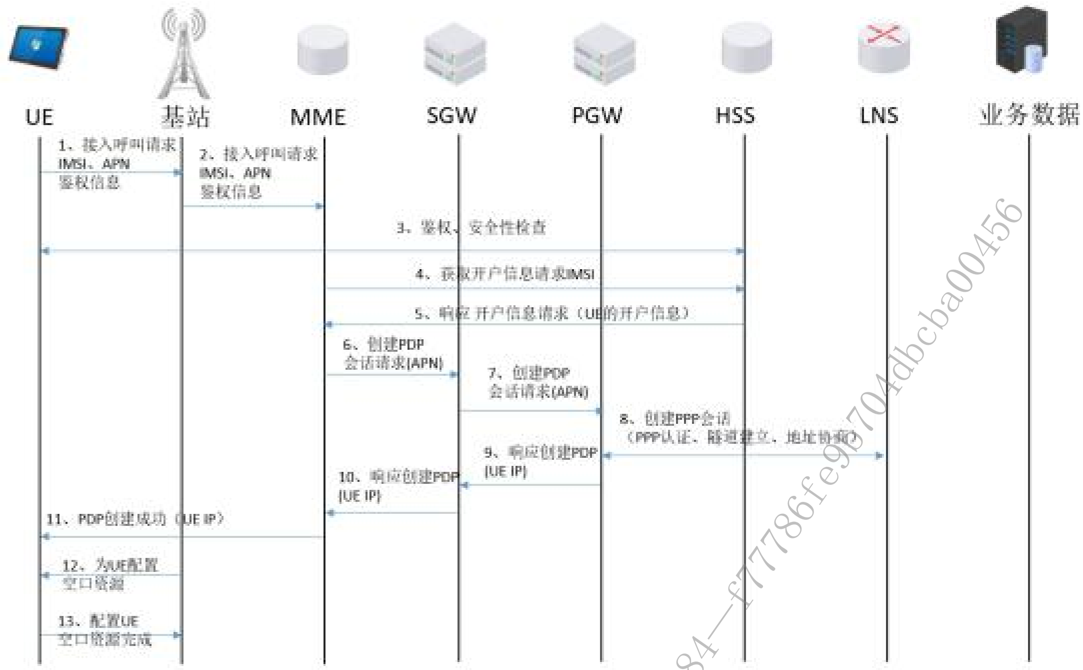
（2）安全可靠

以 L2TP 技术为例，在两端建立安全隧道（Tunnel），通过虚拟专用的通道来传输信息，确保用户通信数据的安全。VPDN 用户通过拨号访问内部网，需经过接入服务器的身份校验，能够有效防止非法访问，便于相关信息的安全管理

（3）数据加密（IPSec）

IPSec 是一组开放的网络安全检查协议的总称，提供访问控制、无连接的完整性、数据来源验证、加密及数据流分类加密等服务。IPSec 在 IP 层提供上述安全服务。IPSec 可用两种方式对数据流进行加密：隧道方式和传输方式。隧道方式对整个 IP 包进行加密，使用一个新的 IPSec 包打包。传输方式仅对数据净荷进行加密，源 IP 包的地址部分不处理。IPSec 支持的组网方式包括：主机与主机、主机与网关、网关与网关。IPSec 可提供对远程访问用户的支持，和 L2TP 隧道协议一起使用，给用户提供更大的安全性和可靠性。

下图为 VPDN 组网原理图：



4G VPDN 组网原理图

客户端 UE 的 4G modem 通过无线信号找到运营商基站并注册连接；

运营商基站携带请求客户端的 IMSI、APN、鉴权信息等发到 MME；

HSS 根据收到的信息对 UE 设备进行鉴权/安全控制；

MME 获取接入设备的信息，如 IMSI 等发送到 HSS 进行鉴权/安全控制处理；

HSS 响应开发信息请求，返回 SGW 的 IP 地址；

MME 向 SGW 发起创建 PDP 会话请求，并传入 APN；

SGW 根据 APN 向 PGW 发起创建 PDP 会话请求；

PGW 收到 SGW 的创建 PDP 会话请求，同时向 LNS 创建 L2TP 隧道，创建 PPP 会话；

PGW 向 SGW 返回创建成功的信息；

SGW 向 MME 返回 PDP 创建成功的信息；

MME 向 UE 返回创建 PDP 会话创建成功的信息；

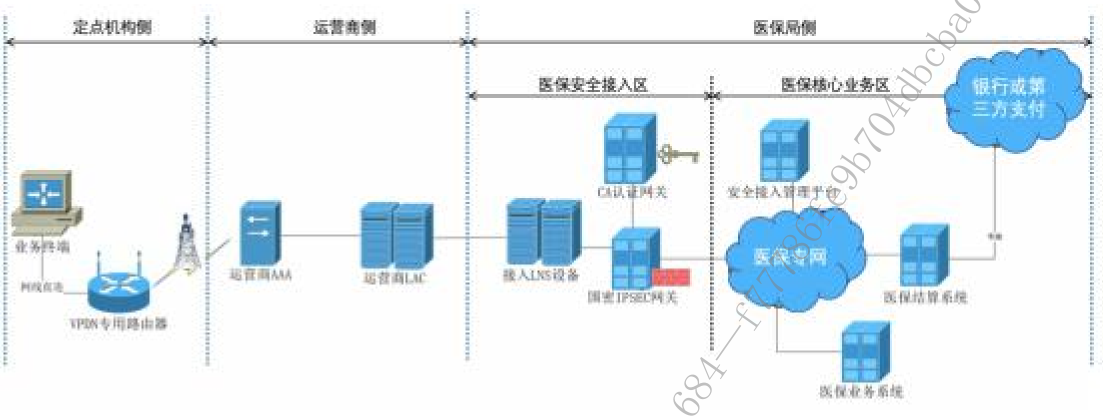
基站为 UE 分配空口资源；

运营商可利用现有 PGW 设备作为 LAC 设备，与医保安全接入区 LNS 设备对接。

2.5 组网场景适配要求

2.5.1 整体部署

海南省组网整体采用省级部署模式，乡镇、村卫生院定点机构的业务终端通过前端的 VPDN 专用路由器，接入移动运营商 4G 网络建立 L2TP 隧道，通过国密网关建立 IPSEC 隧道，最后移动 LNS 设备通过与海南省医保局的互联专线，连通海南省医保局的 CA 认证网关及业务系统，实现乡镇、村卫生院定点机构无线接入终端的认证及数据传输。组网拓扑示意图如下：



采用 4G VPDN 组网方式，所有无线终端设备都处于医疗保障局专用网络内，终端设备直接获取内网 IP 地址。各个关键设备要求如下：

（1）业务终端：手机、笔记本、无线 Modem 等多种设备，

（2）VPDN 专用路由器：具备 VPDN 拨号功能，IPSEC VPN 功能，可对数据链路加密；

（3）专线：通常采用运营商的 100M 以太网专线，此专线将运营商 LAC 设备及医保局 LNS 设备进行连接；

（4）LNS（L2TP Network Server）：医保专用接入 LNS 设备，对接 VPDN 专用路由器；

（5）国密 IPSEC 网关：医保专用 VPN 加密设备，与 VPDN 专用路由器建立国密（SM1/2/3/4）加密隧道；

（6）CA 认证网关：医保专用 CA 认证设备，检验定点机构 SIMkey 内置身份证书合法性。

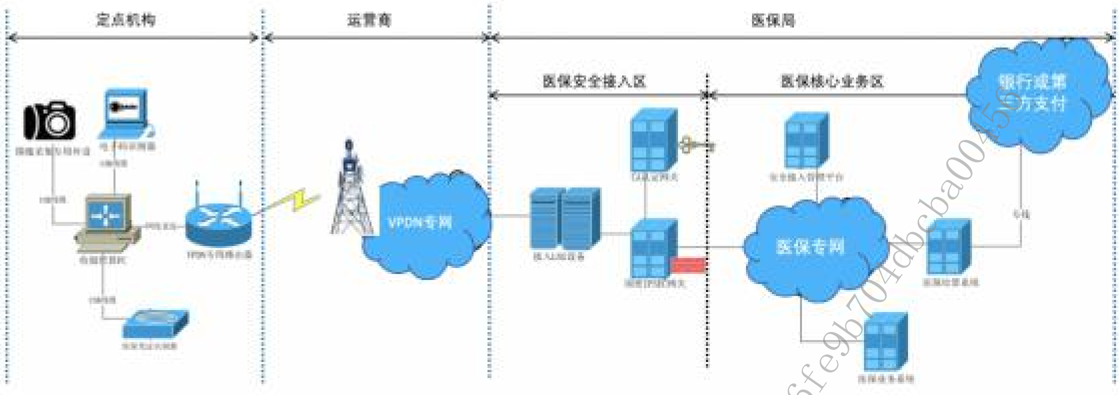
（7）定制物联网卡 SIMkey：定点机构专用 SIM 卡，具备身份证书功能，提供唯一身份标识，作为定点机构入网的唯一凭证；

物联网卡接入要求：

普通物联网卡不可进入运营商医保专网；定制医保物联网卡可到达医保安全接入区；同时具备定制医保物联网卡和医保局电子证书（CA 证书）可以到达医

保核心网，以保障医保通信网络安全。

2.5.2 药店、村卫生室



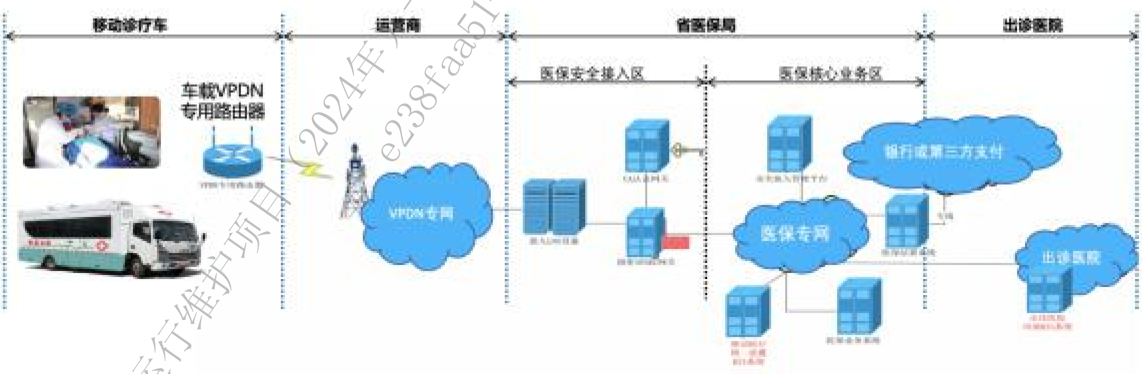
药店、村卫生室建设拓扑

药店、村卫生室接入要求：

接入终端：药店/村卫生室使用原有的收银结算 PC；增加 VPDN 专用路由器；

接入方式：药店/村卫生室原有网络接入部分的设备和线路取消，增加 1 台 VPDN 专用路由器，使用定制的 SIMkey。现在原有收银结算 PC 通过网线与 VPDN 专用路由器连接，VPDN 专用路由器内置 SIMkey，通过内置的相关账户和证书信息，完成鉴权和认证，接入医保专网，完成相关医保业务。

2.5.3 移动诊疗车（预留扩展）



移动诊疗车建设拓扑

移动诊疗车，统一接入到医保专网，使用医保统一的前置 HIS 系统，完成移动诊疗业务。诊疗的电子病历和处方等数据存放到医保局，可按需与出诊医院做数据同步和费用结算。该场景下主要分别为以下 4 个节点，分别为：

（1）移动诊疗车：增加车载 VPDN 专用路由器（含身份识别证书）

（2）运营商：沿用原有 LAC

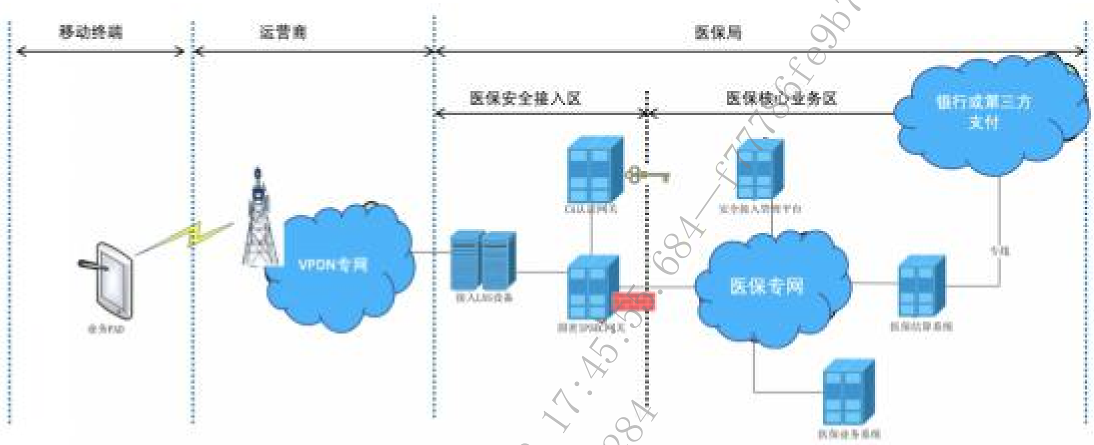
（3）医保局：

构建医保安全接入区，增加 接入 LNS，国密 IPSEC 网关，CA 认证网关；

构建统一前置 HIS 系统，规范移动诊疗，统一移动诊疗相关业务

（4）出诊医院：内部 HIS 系统按照统一接口对接医保局前置 HIS 系统，获取诊疗数据。

2.5.4 远程办公接入（飞行检查）

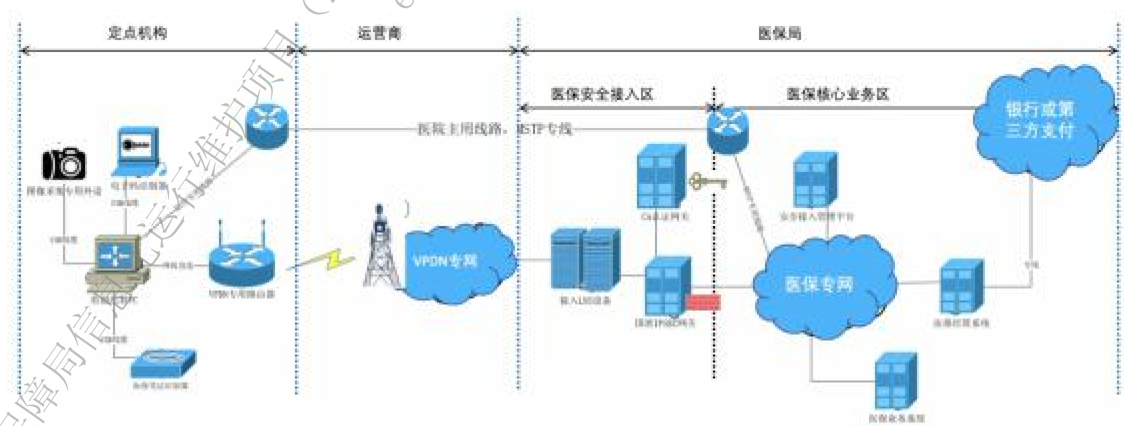


远程办公接入建设拓扑

（1）接入终端：在飞行检查的业务终端增加定制的 SIMkey；

（2）接入方式：飞行检查业务终端插入定制的 SIMkey。通过内置的相关账户和证书信息，完成鉴权和认证，接入医保专网，完成相关医保业务。

2.5.5 医院备份线路



医院备线建设拓扑

医院采用 4G 无线作为备份线路接入医保核心业务区，需保障安全性和可靠

性，要求如下：

（1）接入终端：采用医院原有的缴费窗口终端，该终端通过医院内部局域网连接到医保 VPDN 专用路由器。推荐配比 1 个缴费窗口使用 1 台 VPDN 专用路由器（若流量较小，可考虑 1-5 个缴费窗口配比 1 台 VPDN 专用路由器使用）；

（2）接入方式：VPDN 专用路由器使用 SIMkey 内置的相关账户和证书信息，同运营商和医保局接入设备完成鉴权和认证，安全接入医保专网。

3、接入终端安全性要求

按照国家医疗保障局相关部署要求，定点医药机构需部署 PC 结算终端（可采用原有 PC）及 VPDN 专用路由器终端。其中 VPDN 专用路由器（带国密密码模块和 VPDN 功能），采用定制医保物联网卡和医保局电子证书（CA 证书）进行身份认证和准入。

在定点药店，村卫生室，移动医疗车场景下，部署的 VPDN 专用路由器终端要符合医疗保障部门的安全规范，须满足：

（1）业务终端应按照终端管理规范要求，遵循“一机一密钥，拆机失效”原则

（2）使用的密钥必须在终端的物理结构内部；

（3）业务终端，专机专用，不可与其他业务终端混淆；

（4）开机可用，终端可与各省医保局的 RA 和国家医保局 CA 联动，完成在线证书制作；

（5）在远程办公接入场景下，医保局内部工作人员使用平板电脑或手机终端，应采取以下措施：

（6）应使用专用的 APP 访问医疗保障核心业务区网络。

（7）应采用符合国密算法的加密、沙盒等技术对数据传输和存储进行保护，防止数据泄漏。

（8）采用 VPDN 方式接入，上网卡应与用户绑定，并采取相应技术措施，确保终端只能访问医疗保障核心业务区网络。

（9）终端接入时应使用医疗保障颁发的数字证书进行用户身份认证证书介质可采用 SIM 卡、SD 卡、耳机接口的 USBKEY、蓝牙接口的 USBKEY 等硬件方式。

（10）禁止私自提升终端权限，如获取 root 权限、越狱等。

（11）终端一旦发生遗失，应有相关技术手段防范数据泄露，如远程擦除手段。

4、身份安全要求

应对医疗保障核心业务区网络接入对象进行身份认证。接入用户使用医疗保障部门统一的医疗保障数字证书进行身份认证，接入设备可通过 IP/MAC 地址、设备码、设备证书等进行身份认证。

5、各市县安全区域边界及 VPDN 安全防护

5.1 安全域边界防护

在网络通过采用防火墙技术实现安全域边界访问防护，具体设计如下：
与机房边界防火墙之间部署两台防火墙设备（进行 2：1 虚拟化部署，提供统一管理界面及高性能、高可靠性），实现与核心网的逻辑隔离，同时实现对市县区域内网防病毒、入侵防御等安全防护。

部署的防火墙还应配置以下的安全策略：

（1）会话监控策略：在防火墙配置会话监控策略，当会话处于非活跃一定时间或会话结束后，防火墙自动将会话丢弃，访问来源必须重新建立会话才能继续访问资源；

（2）会话限制策略：对于业务服务器区域边界，从维护系统可用性的角度必须限制会话数，来保障服务的有效性，防火墙可对保护的业务服务器采取会话限制策略，当业务服务器接受的连接数接近或达到阈值时，防火墙自动阻断其他的访问连接请求，避免服务器接到过多的访问而崩溃；

（3）身份认证策略：配置防火墙用户认证功能，对保护的应用系统可采取身份认证的方式（包括用户名/口令方式、USB/KEY 方式等），实现基于用户的访问控制；此外，防火墙能够和第三方认证技术结合起来（包括 RADIUS、TACAS、AD、数字证书），实现网络层面的身份认证，进一步提升系统的安全性，同时也满足 3 级系统对网络访问控制的要求；

（4）日志审计策略：防火墙详细记录了转发的访问数据包，可提供给网络管理人员进行分析。这里应当将防火墙记录日志统一导入到集中的日志管理服务器；

（5）管理员身份认证策略：修改当前防火墙的配置，启用证书认证方式，

以满足网络设备对双因素身份认证的需求。

5.2 实现边界入侵防护

5.2.1 在医保网络中利用防火墙技术，经过仔细的配置，通常能够在安全域之间提供安全的网络保护，降低了网络安全风险，但是入侵者可寻找防火墙背后可能敞开的后门，或者入侵者也可能就在防火墙内。

5.2.2 同时等级保护对三级等级的信息系统也有入侵防范的相关要求：

（1）应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等；

（2）当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。

5.2.3 本方案通过综合采用入侵检测系统和入侵防护技术来实现医保网络的边界入侵防护。

5.2.4 网络入侵检测系统位于有敏感数据需要保护的网络上，通过实时侦听网络数据流，寻找网络违规模式和未授权的网络访问尝试。当发现网络违规行为和未授权的网络访问时，网络监控系统能够根据系统安全策略做出反应，包括实时报警、事件登录，或执行用户自定义的安全策略等。

而入侵防御系统是在线部署在网络中，提供主动的、实时的防护，具备对 2 到 7 层网络的线速、深度检测能力，同时配合以精心研究、及时更新的攻击特征库，即可以有效检测并实时阻断隐藏在海量网络中的病毒、攻击与滥用行为，也可以对分布在网络中的各种流量进行有效管理，从而达到对网络架构防护、网络性能保护和核心应用防护。

5.2.5 具体部署如下：

通过在网络出口部署两台入侵防护系统（通过下一代防火墙开启 IPS 模块）来实现对省政务中心机房的网络攻击的防范，入侵防护系统往往以串联的方式部署在网络中，可以有效检测并实时阻断来自互联网隐藏在海量网络中的病毒、攻击与滥用行为。

5.2.6 这里针对医保网络的入侵防护和入侵检测系统将执行以下的安全策略：

（1）防范网络攻击事件：入侵防护系统采用细粒度检测技术，协议分析技

术，误用检测技术，协议异常检测，可有效防止各种攻击和欺骗。针对端口扫描类、木马后门、缓冲区溢出、IP 碎片攻击等，入侵防护系统可在网络边界处进行监控和阻断。

（2）防范拒绝服务攻击：入侵防护系统在防火墙进行边界防范的基础上，工作在网络的关键环节，能够应付各种 SNA 类型和应用层的强力攻击行为，包括消耗目的端的各种资源如网络带宽、系统性能等攻击，主要防范的攻击类型有 TCP Flood，UDP Flood，SYN Flood，Ping Abuse 等；

（3）审计、查询策略：入侵防护系统能够完整记录多种应用协议（HTTP、FTP、SMTP、POP3、TELNET 等）的内容。记录内容包括，攻击源 IP、攻击类型、攻击目标、攻击时间等信息，并按照相应的协议格式进行回放，清楚再现入侵者的攻击过程，重现内部网络资源滥用时泄漏的保密信息内容。同时必须对重要安全事件提供多种报警机制。

（4）网络检测策略：在检测过程中入侵防护系统综合运用多种检测手段，在检测的各个部分使用合适的检测方式，采取基于特征和基于行为的检测，对数据包的特征进行分析，有效发现网络中异常的访问行为和数据包；

（5）监控管理策略：入侵防护系统提供人性化的控制台，提供初次安装探测器向导、探测器高级配置向导、报表定制向导等，易于用户使用。一站式管理结构，简化了配置流程。强大的日志报表功能，用户可定制查询和报表。

（6）异常报警策略：入侵防护系统通过报警类型的制定，明确哪类事件，通过什么样的方式，进行报警，可以选择的包括声音、电子邮件、消息。

（7）阻断策略：由于入侵防护系统串联在保护区域的边界上，系统在检测到攻击行为后，能够主动进行阻断，将攻击来源阻断在安全区域之外，有效保障各类业务应用的正常开展，这里包括数据采集业务和信息发布业务；

（8）防范网络攻击事件：入侵防护系统采用细粒度检测技术，协议分析技术，误用检测技术，协议异常检测，可有效防止各种攻击和欺骗。针对端口扫描类、木马后门、缓冲区溢出、IP 碎片攻击等，入侵防护系统可在网络边界处进行监控和阻断。

（9）防范拒绝服务攻击：入侵防护系统在防火墙进行边界防范的基础上，工作在网络的关键环节，能够应付各种 SNA 类型和应用层的强力攻击行为，包括

消耗目的端的各种资源如网络带宽、系统性能等攻击，主要防范的攻击类型有 TCP Flood，UDP Flood，SYN Flood，Ping Abuse 等；

（10）审计、查询策略：入侵防护系统能够完整记录多种应用协议（HTTP、FTP、SMTP、POP3、TELNET 等）的内容。记录内容包括，攻击源 IP、攻击类型、攻击目标、攻击时间等信息，并按照相应的协议格式进行回放，清楚再现入侵者的攻击过程，重现内部网络资源滥用时泄漏的保密信息内容。同时必须对重要安全事件提供多种报警机制。

（11）网络检测策略：在检测过程中入侵防护系统综合运用多种检测手段，在检测的各个部分使用合适的检测方式，采取基于特征和基于行为的检测，对数据包的特征进行分析，有效发现网络中异常的访问行为和数据包；

（12）监控管理策略：入侵防护系统提供人性化的控制台，提供初次安装探测器向导、探测器高级配置向导、报表定制向导等，易于用户使用。一站式管理结构，简化了配置流程。强大的日志报表功能，用户可定制查询和报表。

（13）异常报警策略：入侵防护系统通过报警类型的制定，明确哪类事件，通过什么样的方式，进行报警，可以选择的包括声音、电子邮件、消息。

（14）阻断策略：由于入侵防护系统串联在保护区域的边界上，系统在检测到攻击行为后，能够主动进行阻断，将攻击来源阻断在安全区域之外，有效保障各类业务应用的正常开展，这里包括数据采集业务和信息发布业务；

（15）在线升级策略：入侵防护系统内置的检测库是决定系统检测能力的关键因素，因此应定期进行在线升级，确保入侵检测库的完整性和有效性。

5.3 实现边界防病毒

通过在出口部署的防火墙开启防病毒功能模块，在网络层实现对病毒的查杀，分析不同安全区域之间的数据包，对其中的恶意代码进行查杀，防止病毒在网络中的传播。

（1）病毒过滤策略：病毒过滤网关对 SMTP、POP3、IMAP、HTTP 和 FTP 等应用协议进行病毒扫描和过滤，通过恶意代码特征过滤，对病毒、木马、蠕虫以及移动代码进行过滤、清除和隔离，有效地防止可能的病毒威胁，将病毒阻断在敏感数据处理区域之外；

（2）恶意代码防护策略：病毒过滤网关支持对数据内容进行检查，可以采

用关键字过滤，URL 过滤等方式来阻止非法数据进入敏感数据处理区域，同时支持对 Java 等小程序进行过滤等，防止可能的恶意代码进入敏感数据处理区；此外，防火墙也支持对移动代码如 Vbscript、JAVA script、ActiveX、Applet 的过滤，能够防范利用上述代码编写的恶意脚本。

（3）蠕虫防范策略：病毒过滤网关可以实时检测到日益泛滥的蠕虫攻击，并对其进行实时阻断，从而有效防止信息网络因遭受蠕虫攻击而陷于瘫痪。

（4）病毒库升级策略：病毒过滤网关支持自动和手动两种升级方式，在自动方式下，系统可自动到互联网上的厂家网站搜索最新的病毒库和病毒引擎，进行及时的升级。

（5）日志策略：防病毒网关提供完整的病毒日志、访问日志和系统日志等记录，这些记录能够被部署在 3 级计算环境中的日志审计系统所收集。

根据等级保护三级系统技术要求，“主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库”，在产品选型时考虑与主机防病毒不同厂商的产品。

5.4 VPDN 安全防护

（1）数据加密：支持 IPSEC VPN；采用业务需要的安全通信机制；支持国密数字证书读取、识别和校验；支持国密算法链路加密；支持国密 SM2/3/4。

（2）证书对接：支持嵌入适配国家医疗保障系统的 CA 模块，提供关键接口参数。

6、医保专网（含医保云资源）运营保障方案

遵循“医保云”、“医保专网”融合运维原则，运营保障如下：

6.1 运营保障服务

6.1.1 医保专网网络资源管理：资源管理、业务资源监测、业务资源告警/预警及处理上报；网络资源使用周报、月报等；该项管理能力要求扩展到医保云资源管理，形成医保专网和医保云基于统一平台的运营保障机制；

6.1.2 功能：服务商医保专网网络资源管理兼顾医保云资源管理，应具备管理平台，其功能应满足以下要求：

（1）资源可视化：一切资源信息化、信息目录化、目录全局化、全局标准化。从全局到局部，从面到点，逐步深入、层层递进。系统拓扑架构可视化：对网络拓扑、主机拓扑、虚拟化拓扑、业务拓扑可视化，实现对各类系统架构拓扑

一目了然，发现业务瓶颈、定位故障根源。对医保云资源实时监测，发现资源不足、性能不足并对趋势预判、预警，提交驻场的运营保障团队及时处置。

（2）提供对医保专网（含医保云）资产、备品备件全生命周期的资产管理。如：采购进度、维修进展、维保到期提醒。

（3）系统安全感知：对医保专网中各个节点的流量和安全数据进行采集，以大数据分析为基础，全面感知安全态势，实现安全架构从被动防御到主动防御的升级，达到从局部安全提升为全局安全、从单点预警提升为协同预警、从模糊管理提升为量化管理的效果。

（4）兼顾医保云运维管理：对应用、服务器、网络、PC、以及数据备份等实现全方位多角度运维监控；工单池报修量，工程师在岗/休假、工作繁忙程度、正在处理的事情等；对 IT 运维各类知识、解决方案的积累。

（5）大屏展现：建立驾驶舱主框架，包括待办支持、关键性能指标、专题分析框架、常用功能。提供业务专题分析、资源专题分析、运维专题分析等各类辅助决策数据。

6.2 人员驻点服务

6.2.1 医保专网（含医保云）运营管理

（1）协助医保局对医保专网资源的新增、封停、解封、扩容、撤收等进行申报、审批并协助处置；对医保云资源进行申报、审批、分配调整、停用释放等管理与处置；

（2）经过局方授权，收集承建商对医保专网（含医保云）资源的需求，向运营商提交带宽扩容、开通和停用申请与处置，向政务云申报云资源增减报告并协调实施；

（3）对医保专网（含医保云）资源人工巡检、点检；并由运营服务人员提供巡检周报、月报，对医保专网（含医保云）资源的使用情况进行监测，提出告警、预警；提出分配调整、停用释放等建议方案，并负责与维保团队协同处置；

（4）经过局方授权，协助实施接入终端设备管控：新增终端设备、停用终端设备；

（5）对运营商承担的医保专网网络资源及其安全防护进行巡检、点检，并提供巡检周报、月报。发现问题后及时提交运营商，并协助处置。驻场人员每月

提交一次联网质量分析报告和网络安全报告；

（6）协助制定医保专网（含医保云）运营制度。

6.2.2 医保信息化系统运营保障

（1）经过局方授权，根据用户日常维护规定，管理医保信息化系统各软件系统的超级管理员账号、密码，定期更换密码；对必须通过 VPN 或远程桌面进行维护的操作，进行维护审计；

（2）经过局方授权，管理医保信息化系统各软件系统的数据库账号、密码，定期更换密码；登记承建商对数据库访问的人工操作申请并记录结果；

（3）根据业务运营需要，对业务数据收集、入库等进行监管、协调；

（4）完成用户指定的医保信息化系统运营的其他任务。

（5）协助制定医保信息化系统运营制度

6.2.3 医保专网（含医保云）运营管理及医保信息化系统运营保障驻场人员要求：

（1）驻场人员不少于 4 人，工作时间为：7 天*8 小时/周；

（2）人员要求；具有相应专业资质和运维经验；人员需要通过局方面试；

（3）驻点人员需包含现场服务项目经理 1 名：需要具备 PMP（项目管理专业人士资格认证）专业资质；

6.2.4 “村医通”便民服务工程终端接入管控服务：

“村医通”POS 机配套 4G 卡联网组网，网络安全保障、链路加密、终端接入管控、联网质量保障等配套服务，

四、关键服务说明

1、定期巡检服务

1.1 服务内容描述

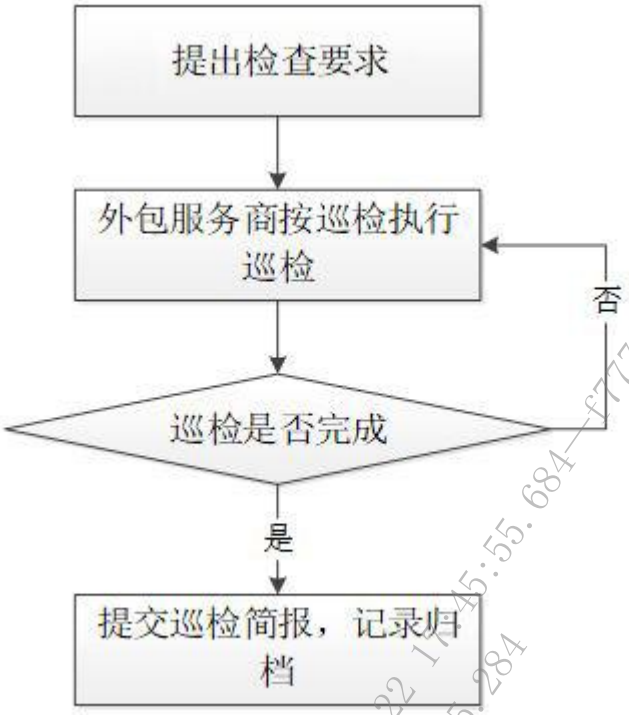
系统维护是以预防为主，运维服务商安排工程师对本项目的设备进行定期（按季度）检查机房环境，供电系统，设备软硬件运行情况、系统性能和物理连接等指标，及早发现故障隐患，减少系统宕机的机会，优化运行环境，延长设备寿命。

每次巡检结束，运维服务商现场工程师填写“定期巡检表”，海南省医疗保障局信息办的技术人员确认后签字。“定期巡检表”一式两份，海南省医疗保障

局信息办和运维服务商各存一份，最终出具正式的巡检总结报告。

1.2 服务流程要求

运维服务商应按以下流程制定严格的定期健康检查流程：



2、现场故障处理服务

2.1 服务内容

主要服务内容包括：

（1）对于清单上的设备，根据故障现象，提供现场故障诊断，快速定位故障原因；

（2）进行 7×24 小时不间断故障处理，直至业务恢复；

（3）在设备出现硬件故障，需要更换时，运维服务商需提供备件保修服务；

（4）必要时触发故障升级管理流程；

（5）故障处理过程中，由服务热线通知故障申告人处理进展和状态；

（6）故障处理完毕后，由服务热线通知故障申告人确认，并做满意度调查，闭环管理。

2.2 故障等级

故障等级划分表

序号	故障等级	故障现象

1	P1 级	系统宕机或者不可用，不能保存进行中的工作，或者导致数据丢失等，导致对应的业务服务停止
2	P2 级	系统严重告警或性能明显下降，业务系统不正常使用，导致对应的业务服务受到影响等
3	P3 级	系统出现一般告警，或性能有所下降，对应的业务服务能够提供

2.3 故障管理

为了保证服务质量指标得以实现，需设置了故障升级管理制度，运维服务商应与设备和服务提供商建立密切的合作和沟通关系，在必要时可以组织各方面的专家，共同解决复杂疑难故障。

如果需要，运维服务商的管理层直接参与设备的维护服务，调度及整合更多资源，快速制定解决方案、监督解决过程，使故障得以快速、妥善地解决。

3、问题管理与记录服务

资料管理是维护工作的基石，运维服务商需在海南省医疗保障局信息办许可的情况下，建立服务维护档案，以便在需要时可以快捷准确的查询。

服务内容如下：

3.1 服务记录：将提供服务记录和服务简报，包括热线服务记录，现场故障服务记录，专项服务记录，备件服务记录等，各项记录一式两份；定期向海南省医疗保障局提供服务简报，包括月度、半年和年度服务简报，将服务工作和维护建议定期向海南省医疗保障局汇报。

3.2 分析报告服务：在每次故障处理结束后，都会向海南省医疗保障局提供故障分析报告服务；在海南省医疗保障局有需求时，提供系统性能分析报告、优化建议报告，变更分析报告等服务。负责对各种报告分类归档管理，方便查阅。

3.3 服务结束后，提交运行维护服务报告，将服务期内的日常巡检记录、各种故障处理情况、设备运行情况、设备健康状况详细记录，并根据海南省医疗保障局业务实际情况对各系统进行全面的评估，并提出优化和未来发展建议。

五、商务要求

1、服务期限：2024 年 5 月 1 日至 2024 年 12 月 31 日。

2、交付地点：用户指定地点。

3、交付方式：免费送至用户指定地点。

4、采购资金的支付方式、时间、条件：

4.1 合同签订后，乙方按甲方要求，提供正式有效用于支付合同价款所需的增值税普通发票和资料，甲方自收到上述增值税普通发票和资料之日起 15 个工作日内支付乙方合同总额的 40%。

4.2 乙方应按甲方要求委托第三方机构根据乙方实际开通电路进行清算，清算产生的额外费用由乙方承担；乙方应在项目服务期满 15 个工作日内出具最终结算报告（以实际电路开通及使用情况的日历天计算，计算方式为：电路单价*实际使用计费天数/365 天）。甲方根据乙方提交的结算报告及验收材料确认最终合同结算金额后 15 个工作日内组织验收。验收通过后 30 个工作日内，甲乙双方根据双方确定的最终合同结算总额，结合合同已付金额，以多退少补的形式进行最终结算并完成支付。

4.3 本项目自 2024 年 5 月 1 日起至乙方完成本项目部署期间是由中国移动通信集团海南有限公司向甲方提供服务。本合同生效且乙方完成本项目部署后，乙方须按合同约定的计价方式在 15 个工作日内与中国移动通信集团海南有限公司办理 2024 年 5 月 1 日起至乙方完成部署期间的费用结算，具体结算细节由乙方与中国移动通信集团海南有限公司协商，甲方不承担任何给付责任。

5、验收要求：按标书服务要求和国家行业标准进行验收。

6、其他要求：服务商应确保网络畅通且网络连接到位。若由于乙方责任，导致甲方维护设备出现大规模断网，出现一次扣除合同总价的 5%，以此类推，最高扣除 15%，甲方有权终止合同。（若非乙方责任的，由乙方进行自证。此外以上提到的大规模断网指的是一个及以上地级市或两个及以上县级市出现一小时以上断网）（提供承诺函加盖公章）

D 包：等级保护测评服务

一、项目名称

海南省医疗保障局信息化运行维护项目（2024 年）

标包名称：等级保护测评服务

二、项目服务要求

1、 网络安全等保服务要求

网络安全等级保护测评是测评机构依据国家网络安全等级保护制度规定，受海南省医疗保障局的委托，按照有关管理规范和技术标准，运用科学的手段和方法，对非涉及国家秘密的网络安全等级保护对象，采用安全技术测评和安全管理测评方式，对保护状况进行检测评估，判定被测对象的技术和管理级别与所定安全等级要求的符合程度，基于相关判定标准给出是否满足所定安全等级的结论，针对安全不符合或部分符合项提出安全整改建议，是网络安全等级保护工作的重要环节。

目前，海南省医疗保障局医疗保障信息平台二期建设工程和“村医通”便民服务工程的等级报告定级备案工作已完成。将按照国家有关规定和标准规范要求，委托专业的测评机构对系统进行等保咨询和测评，从技术和管理两大方面发现系统中的安全问题，以便及时消除或降低安全风险。

清单如下：

医疗保障信息平台二期建设工程：

序号	信息系统名称	安全保护等级	定级备案情况	等保测评情况	本次等保测评要求
1	核心业务平台及业务中台	三级	已完成	每年一次	每年一次
2	智慧医保数据业务平台	三级	已完成	每年一次	每年一次
3	公共服务系统平台	三级	已完成	每年一次	每年一次
4	医保业务终端	三级	已完成	每年一次	每年一次

1.1 等保测评服务内容和流程

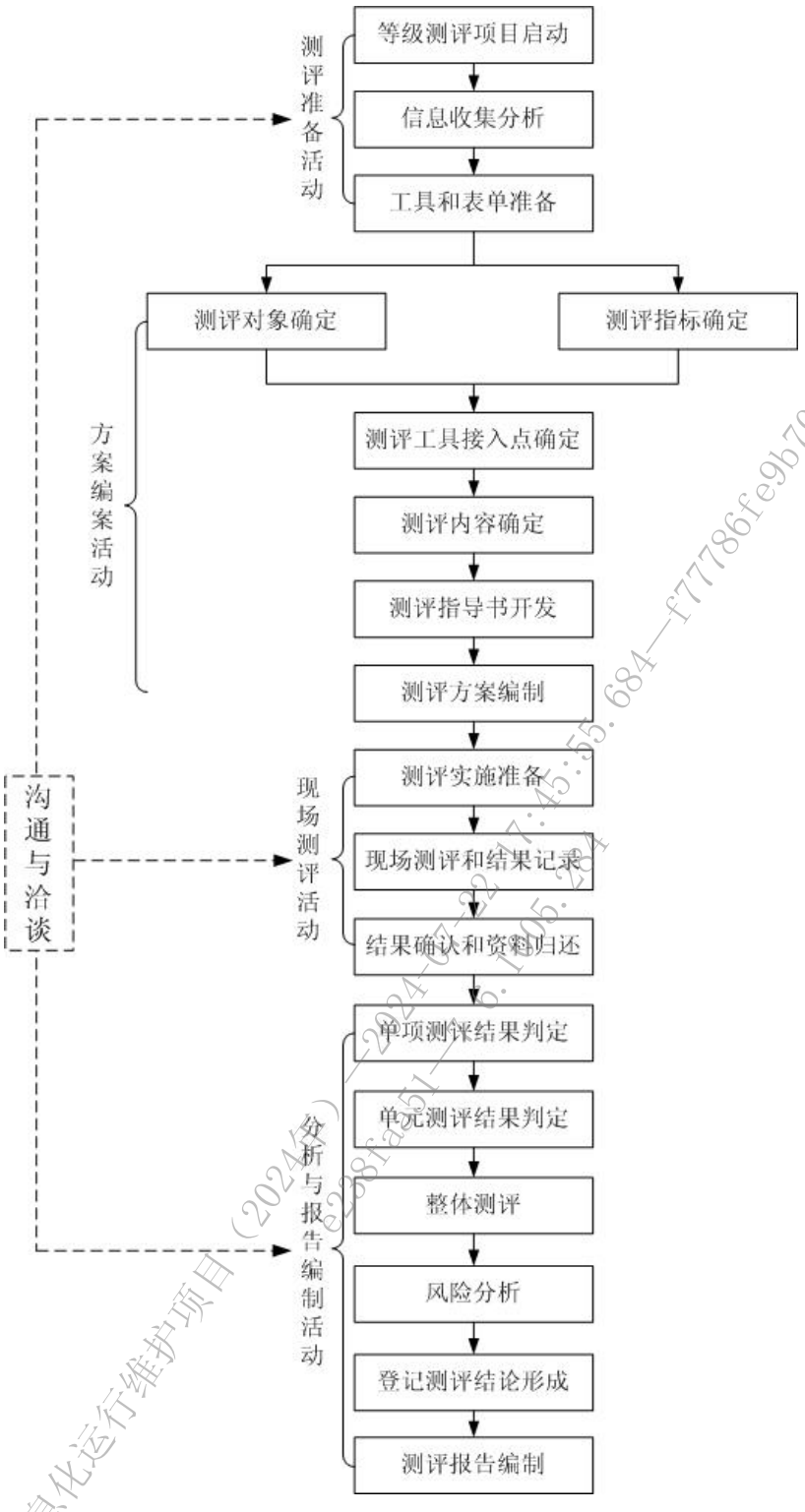
1.1.1 测评内容

委托符合国家要求的专业机构依据《信息系统安全等级保护基本要求》，落

实物理安全、网络安全、主机安全、应用安全和数据安全等安全保护技术措施，落实安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理等安全保护管理措施，具体内容如下图所示：

1.1.2 测评流程

对信息系统等级保护测评实施的基本流程见图：



为确保等级测评工作的顺利开展，应首先明确等级测评的工作流程，然后按照工作流程中的活动内容有序地开展等级测评工作。由于不同安全保护等级信息系统的重要程度不同，安全保护力度不同，从国家等级保护的角度出发，等级测评的关注角度也应有所差异。

等级测评过程可以分为四个活动内容：测评准备活动、方案编制活动、现场

测评活动和分析与报告编制活动，而测评双方之间的沟通与洽谈应贯穿整个等级测评过程。在方案编制活动中，测评对象确定和测评指标确定两项任务可以并行。

测评成果为：《信息系统等级测评报告》。其构成如下：

序号	任务	输出文档	文档内容
1	单项测评结果判定	等级测评报告的等级测评结果记录部分	分析测评对象的安全现状与标准中相应等级基本要求项的符合情况，给出单项测评结果和符合程度得分
2	单元测评结果判定	等级测评报告的单元测评小结部分	汇总统计单项测评结果，分析计算控制点符合情况、存在的安全问题
3	整体测评	等级测评报告的整体测评部分	分析被测定级对象整体安全状况及对单项测评结果的影响情况，给出安全问题严重程度及对应的要求项符合程度得分修正值
4	系统安全保障评估	测评报告的系统安全保障评估部分	汇总被测定级对象已采取的安全保护措施情况，计算安全控制点得分及安全层面得分，并总体评价被测定级对象已采取的有效保护措施和存在的主要安全问题情况
5	安全问题风险分析	等级测评报告的安全问题风险评估部分	分析被测定级对象存在安全问题可能对定级对象、单位、社会及国家造成的最大安全危害（损失），并给出风险等级
6	等级测评结论形成	等级测评报告的等级测评结论部分	对测评结果进行分析，形成等级测评结论，并给出综合得分
7	测评报告编制	经过评审和确认的被测定级对象等级测评报告	等级测评结果记录，单元测评结果汇总及结果分析，整体测评过程及结果，风险分析过程及结果，等级测评结论，问题处置建议等

1.2 网络安全等级保护测评指标

（1）安全物理环境

（2）安全通信网络

（3）安全区域边界

（4）安全计算环境

（5）安全管理中心

（6）安全管理制度

（7）安全管理机构

（8）安全管理人员

（9）安全建设管理

（10）安全运维管理

1.3 等保测评范围

按照业务条线归并，本项目对以下 4 大业务类评：

（1）核心业务平台及业务中台（三级）

（2）智慧医保数据业务平台（三级）

（3）公共服务系统平台（三级）

（4）医保业务终端（三级）

表 5-1 信息系统清单

序号	信息系统名称	分类
1	业务中台子系统	核心业务平台及业务中台
2	统一门户子系统	
3	基础信息管理子系统	
4	医疗服务价格管理子系统	
5	医保业务基础子系统	
6	跨省异地就医子系统	
7	报表管理子系统	
8	数据治理数字化管理平台	
9	医保药品“双通道”管理信息系统	
10	需求管理平台	

序号	信息系统名称	分类
11	药品和医用耗材招采系统	
12	支付方式管理子系统	
13	分组付费子系统	
14	海南省医疗服务价格监测	
15	智能监管子系统	智慧医保数据业务平台
16	基金运行及审计监管子系统	
17	内部控制子系统	
18	医保管家子系统	
19	全生命周期档案子系统	
20	综合统计分析子系统	
21	宏观决策大数据系统	
22	信用评价子系统	
23	公共服务子系统	公共服务系统平台
24	药品和医用耗材招采系统	
25	海南医保村医通	医保业务终端
26	医保业务终端	

1.4 网络安全等级保护测评结果处置

根据网络安全等级保护测评发现的问题，提供整改方案，由业主方责成承建方、运维方根据各自合同的责任进行整改，提交整改报告及测试报告，直至完成。

三、商务要求

1、服务期限：

（1）2024 年度。

（2）合同签订并完成定级备案且收到甲方测评通知后 60 天内完成“网络安全等级保护等级测评服务、网络安全等级保护安全建设整改设计”。

（3）合同签订后，乙方需按照甲方要求免费提供 1 次网络安全现场培训，开展 2 次以上网络安全线上培训。

2、项目的实施要求

2.1 测评项目实施过程中，投标人应遵循国家标准、行业标准。

2.2 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，测评单位需安排驻场人员开展测评工作，排查测评问题，协助采购人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。

2.3 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。

（1）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。

（2）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。

2.4 项目验收标准和方式

（1）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。

（2）技术服务工作成果：

①根据甲方需求阶段性提交工作报告，内容包含进展情况、存在问题及下一步计划。

②验收阶段，须提交 4 份《网络安全等级保护测评报告》作为验收成果，并根据项目情况提供验收及备案所需的纸质文件及电子版文件（刻光盘）。

（3）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。

（4）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。

2.5 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。

3、采购资金的支付方式、时间、条件：

3.1 合同签订后 10 个工作日内，甲方凭乙方开具的合法有效与本次支付价款等额的发票以银行转账方式向乙方支付合同金额的 50%。

3.2 乙方提交的所有技术成果经甲方验收合格后 10 个工作日内，甲方凭乙方开具的合法有效与本次支付价款等额的发票以银行转账方式向乙方支付合同金额的 50%。

E 包：商用密码应用安全性评估服务

一、项目名称

海南省医疗保障局信息化运行维护项目（2024 年）

标包名称：商用密码应用安全性评估服务

二、项目服务内容

1、密码应用安全性评估服务方案

依据《信息系统密码应用基本要求》(GM/T0054-2018)、《信息系统密码测评要求（试行）》《商用密码应用安全性评估测评过程指南（试行）》《商用密码应用安全性评估测评作业指导书（试行）》《关于进一步明确省政务信息化项目建设密码应用有关要求的通知（琼国密局字〔2021〕2 号）》和系统自身的安全需求，对医疗保障信息平台二期建设工程应用系统和“村医通”应用系统进行商用密码应用安全性评估，为重要信息系统的密码安全提供科学评价，逐步规范网络运营者的密码使用和管理行为。清单如下：

表 5- 2 密码应用评估服务情况

序号	信息系统分类	密码应用安全性评估情况	本次密码应用安全评估要求
1	核心业务平台及业务中台	每年一次	每年一次
2	智慧医保数据业务平台	每年一次	每年一次
3	公共服务系统平台	每年一次	每年一次
4	医保业务终端	每年一次	每年一次

信息系统清单如下：

表 5- 3 信息系统清单

<table>
<tr><th>序号</th><th>信息系统名称</th><th>分类</th></tr>
<tr><td>1</td><td>业务中台子系统</td><td rowspan="6">核心业务平台及业务中台</td></tr>
<tr><td>2</td><td>统一门户子系统</td></tr>
<tr><td>3</td><td>基础信息管理子系统</td></tr>
<tr><td>4</td><td>医疗服务价格管理子系统</td></tr>
<tr><td>5</td><td>医保业务基础子系统</td></tr>
<tr><td>6</td><td>跨省异地就医子系统</td></tr>
</table>

7	报表管理子系统	
8	数据治理数字化管理平台	
9	医保药品“双通道”管理信息系统	
10	需求管理平台	
11	药品和医用耗材招采系统	
12	支付方式管理子系统	
13	分组付费子系统	
14	海南省医疗服务价格监测	
15	智能监管子系统	智慧医保数据业务平台
16	基金运行及审计监管子系统	
17	内部控制子系统	
18	医保管家子系统	
19	全生命周期档案子系统	
20	综合统计分析子系统	
21	宏观决策大数据系统	
22	信用评价子系统	
23	公共服务子系统	公共服务系统平台
24	药品和医用耗材招采系统	
25	海南医保村医通	医保业务终端
26	医保业务终端	

1.1 密码应用总体测评

1.1.1 密码算法测评。信息系统中使用的密码算法是否符合法律法规的规定和密码相关国家标准、行业标准的有关要求。

1.1.2 密码技术测评。信息系统中使用的密码技术是否遵循密码相关国家标准和行业标准。

1.1.3 密码产品测评。信息系统中使用的密码产品是否符合国家法律和国家密码管理部门的有关规定。

1.1.4 密钥管理测评。对密钥的生成、存储、分发、导入、导出、使用、备

份、恢复、归档与销毁等环节进行管理和策略制定的全过程是否符合要求。

1.1.5 安全管理测评。对制度、人员、实施和应急等四个方面安全管理的测评，并协助完善商用密码应用安全性管理制度，协助完善密码相关系统运维管理制度。

1.2 密码技术应用测评

1.2.1 物理和环境安全

需密评单位负责协助海南省医疗保障局协调大数据管理局推进信息系统密评工作。

1.2.2 网络和通信安全测评

核心网络由医保局协调，向大数据局提出密评管理要求；对外延伸网络由医保局主责，中标单位负责协助医保局完成对外延伸网络密评工作。

医保局负责对外延伸的网络和通讯安全，主要分为两个区的对外安全，核心业务区的访问入口主要包括网站和智能终端。对于实现有线连接的经办机构、定点医疗机构使用网站接入，对于电子政务外网暂时无法覆盖的经办机构，暂时未能实现有线接入的定点医疗机构使用 VPDN+4/5G+智能终端的方式接入。公共服务区的访问入口支持多种渠道的访问，具体包括国家平台访问入口、海南省政务服务网访问入口、医保局网站、自助终端、小程序、互联网企业等第三方渠道等。

1.2.3 设备和计算安全测评

需密评单位负责协助海南省医疗保障局协调大数据管理局推进信息系统密评工作。

1.2.4 应用和数据安全测评

（1）是否使用密码技术对登录的用户进行身份标识和鉴别，实现身份鉴别信息的防截获、防假冒和防重用，保证应用系统用户身份的真实性；

（2）是否使用密码技术的完整性功能来保证业务应用系统访问控制策略、数据库表访问控制信息和重要信息资源敏感标记等信息的完整性；

（3）是否采用密码技术保证重要数据在传输过程中的机密性，包括但不限于鉴别数据、重要业务数据和重要用户信息等；

（4）是否采用密码技术保证重要数据在存储过程中的机密性，包括但不限于鉴别数据、重要业务数据和重要用户信息等；

（5）是否采用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用户信息等；

（6）是否采用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用户信息、重要可执行程序等；

（7）是否使用密码技术的完整性功能来实现对日志记录完整性的保护；

（8）是否采用密码技术对重要应用程序的加载和卸载进行安全控制；

（9）是否采用符合 GM/T 0028 的三级及以上密码模块或通过国家密码管理部门核准的硬件密码产品实现密码运算和密钥管理。

1.3 密钥管理测评

检测信息系统密钥管理各环节，包括对密钥的生成、存储、分发、导入、导出、使用、备份、恢复、归档与销毁等环节进行管理和策略制定的全过程是否符合要求。

1.3.1 密钥生成

密钥生成使用的随机数是否符合 GM/T 0005 要求，密钥是否在符合 GM/T 0028 的密码模块中产生；密钥是否在密码模块内部产生，不得以明文方式出现在密码模块之外；是否具备检查和剔除弱密钥的能力。

1.3.2 密钥存储

密钥是否加密存储，并采取严格的安全防护措施，防止密钥被非法获取；加密密钥是否存储在符合 GM/T 0028 的二级及以上密码模块中。

1.3.3 密钥分发

密钥分发是否采取身份鉴别、数据完整性、数据机密性等安全措施，是否能够抗截取、假冒、篡改、重放等攻击，保证密钥的安全性。

1.3.4 密钥导入与导出

是否采取安全措施，防止密钥导入导出时被非法获取或篡改，并保证密钥的正确性。

1.3.5 密钥使用

密钥是否明确用途，并按用途正确使用；对于公钥密码体制，在使用公钥之

前是否对其进行验证；是否有安全措施防止密钥的泄露和替换；密钥泄露时，是否停止使用，并启动相应的应急处理和响应措施。是否按照密钥更换周期要求更换密钥；是否采取有效的安全措施，保证密钥更换时的安全性。

1.3.6 密钥备份与恢复

是否制定明确的密钥备份策略，采用安全可靠的密钥备份恢复机制，对密钥进行备份或恢复；密钥备份或恢复是否进行记录，并生成审计信息；审计信息包括备份或恢复的主体、备份或恢复的时间等。

1.3.7 密钥归档

是否采取有效的安全措施，保证归档密钥的安全性和正确性；归档密钥只能用于解密该密钥加密的历史信息或验证该密钥签名的历史信息；密钥归档是否进行记录，并生成审计信息；审计信息包括归档的密钥、归档的时间等；归档密钥是否进行数据备份，并采用有效的安全保护措施。

1.3.8 密钥销毁

是否具有在紧急情况下销毁密钥的措施。

1.4 安全管理测评

对制度、人员、实施和应急等四个方面安全管理的测评，并协助完善商用密码应用安全性管理制度，协助完善密码相关系统运维管理制度。

1.4.1 制度

（1）是否制定密码安全管理制度及操作规范、安全操作规范。密码安全管理制度是否包括密码建设、运维、人员、设备、密钥等密码管理相关内容；

（2）是否定期对密码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；

（3）是否明确相关管理制度发布流程。

1.4.2 人员

（1）是否了解并遵守密码相关法律法规；

（2）是否能够正确使用商用密码产品；

（3）是否根据相关密码管理政策、数据安全保密政策，结合组织实际情况，设置密钥管理人员、安全审计人员、密码操作人员等关键岗位；建立相应岗位责任制度，明确相关人员在安全系统中的职责和权限，对关键岗位建立多人共管机

制；密钥管理、安全审计、密码操作人员职责，互相制约互相监督，相关设备与系统的管理和使用账号不得多人共用；

（4）是否建立人员考核制度，定期进行岗位人员考核，建立健全奖惩制度；

（5）是否建立人员培训制度，对于涉及密码的操作和管理以及密钥管理人员进行专门培训；

（6）是否建立关键岗位人员保密制度和调离制度，签订保密合同，承担保密义务。

1.4.3 实施

（1）规划

信息系统规划阶段，责任单位是否依据密码相关标准，制定密码应用方案，组织专家进行评审，评审意见作为项目规划立项的重要材料。

通过专家审定后的方案是否作为建设、验收和测评的重要依据。

（2）建设

是否按照国家相关标准，制定实施方案，方案内容是否包括但不少于信息系统概述、安全需求分析、商用密码系统设计方案、商用密码产品清单（包括产品资质、功能及性能列表和产品生产单位等）、商用密码系统安全管理与维护策略、商用密码系统实施计划等。

是否选用的经国家密码管理部门核准的密码产品、许可的密码服务。

（3）运行

信息系统投入运行前，是否经密码测评机构进行安全性评估，评估通过方可投入正式运行。

信息系统投入运行后， 责任单位每年是否委托密码测评机构开展密码应用安全性评估，并根据评估意见进行整改；有重大安全隐患的，是否停止系统运行，制定整改方案，整改完成并通过评估后方可投入运行。

1.4.4 应急

（1）是否制定应急预案，做好应急资源准备，当事件发生时，按照应急预案结合实际情况及时处置；

（2）事件发生后，是否及时向信息系统的上级主管部门进行报告；

（3）事件处置完成后，是否及时向同级的密码主管部门报告事件发生情况

及处置情况。

1.5 形成密码应用安全性评估相关报告

针对每个被评估系统编制密码应用安全性评估报告，报告按照国家密码管理局要求包含的内容编制。协助被评估单位认清风险，查找漏洞，找出差距，提出有针对性的加强完善密码安全管理和防护建议。

1.6 密码应用安全性评估范围

2023 年报备 9 个系统按照业务条线归并，本项目对以下 4 大业务类进行密码应用安全性评估：

（1）核心业务平台及业务中台（三级）

（2）智慧医保数据业务平台（三级）

（3）公共服务系统平台（三级）

（4）医保业务终端（三级）

信息系统清单如下：

序号	信息系统名称	分类
1	业务中台子系统	核心业务平台及业务中台
2	统一门户子系统	
3	基础信息管理子系统	
4	医疗服务价格管理子系统	
5	医保业务基础子系统	
6	跨省异地就医子系统	
7	报表管理子系统	
8	数据治理数字化管理平台	
9	医保药品“双通道”管理信息系统	
10	需求管理平台	
11	药品和医用耗材招采系统	
12	支付方式管理子系统	
13	分组付费子系统	
14	海南省医疗服务价格监测	

15	智能监管子系统	智慧医保数据业务平台
16	基金运行及审计监管子系统	
17	内部控制子系统	
18	医保管家子系统	
19	全生命周期档案子系统	
20	综合统计分析子系统	
21	宏观决策大数据系统	
22	信用评价子系统	
23	公共服务子系统	公共服务系统平台
24	药品和医用耗材招采系统	
25	海南医保村医通	医保业务终端
26	医保业务终端	

三、商务要求

1、服务期限：2024 年度。

2、项目实施要求

2.1 项目管理要求

（1）合同签订后，测评单位需安排驻场人员开展测评工作，排查测评问题，协助采购人指导系统承建方完成问题整改工作。

（2）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；

（3）成交方为本项目实施期间提供现场不少于 3 人的 项目实施团队（包含 1 名项目经理），该团队的核心技术人员应参加国家密码管理局统一组织的培训，通过商用密码应用安全性评估能力考核；

（4）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，项目实施应依据商用密码应用安全性评估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。

（5）乙方须在 2024 年 11 月底前完成密码应用安全性评估工作，并协助甲方完成整改工作。

2.2 技术文件要求

开展安全测评过程中，成交方应按照要求形成全面详尽的技术资料，包括但不限于：

（1）项目计划书

（2）密码测评方案

（3）现场测评实施计划

（4）测评记录表

（5）测评整改方案

（6）整改报告

（7）测评报告

验收后调整和补充的项目成果和资料，确保技术资料的一致性、完整性和真实性，并向采购人提交审核。

2.3 项目验收标准与要求

按照《商用密码应用安全性评估管理办法（试行）》《信息系统密码应用基本要求》（GB/T39786-2021）《信息系统密码测评要求（试行）》《信息系统密码应用测评要求（试行）》《商用密码应用安全性评估测评过程指南（试行）》《商用密码应用安全性评估测评作业指导书（试行）》等要求，成交供应商在项目终验前为甲方提供工程项目的商用密码应用安全性评估报告，作为项目验收的依据之一，并协助甲方将评估结果报海南省密码管理部门成功备案。

2.4 保密要求

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。

3、采购资金的支付方式、时间、条件：本项目经费采用两次付款支付方式。

3.1 合同签订生效后，甲方凭乙方提供的合法有效且与本次支付价款等额的发票，在 10 个工作日内向乙方支付合同总价的 50%。

3.2 乙方完成项目服务内容，并指导承建单位完成系统整改且通过甲方组织的验

收后，甲方凭乙方提供的合法有效且与本次支付价款等额的发票，在 10 个工作日内向乙方支付合同总价的 50%。