

合同编号：

鹤壁市医疗保障大数据反欺诈数据服务项目合同

甲方：鹤壁市医疗保障局

法定代表人：王永军

地址：鹤壁市淇滨区黄河路366号

电话：0392-3365366

乙方：鹤壁豫信电子科技有限公司

法定代表人：陈炜鑫

注册地址：鹤壁市淇滨区珠江路与淇水大道交叉口龙门大厦A座三楼

合同联系人：田文玺

电子邮箱：tianwenxi@cathink.com.cn

鹤壁市医疗保障局（以下称甲方）确定鹤壁豫信电子科技有限公司（以下称乙方）作为鹤壁市医疗保障大数据反欺诈数据服务项目（以下简称“本项目”或“项目”）的建设服务商，为甲方提供本项目所需平台建设、实施等技术服务。乙方同意作为甲方鹤壁市医疗保障大数据反欺诈数据服务项目的建设服务商，为甲方提供本项目所需平台建设、实施等技术服务。

双方经过平等协商，在真实、充分地表达各自意愿的基础上，根据《中华人民共和国民法典》的规定，达成如下合同条款，并由双方共同恪守。

一、项目服务内容

提供市医疗保障大数据反欺诈数据服务（包括反欺诈数据专区、医保反欺诈大数据模型、监测中心、反欺诈智慧驾驶舱等）。产品功能清单及分项报价详见附件。

二、工期

项目工期：自合同签订起110日历天。

三、合同价格及付款方式

1、合同价格

双方约定本项目合同含税总金额为：人民币¥2650000.00元（大写：贰佰陆拾伍万元整），税率是6%和13%（详细税率见附件），其中不含税价为：人民币 ¥2454416.43元（大写：贰佰肆拾伍万肆仟肆佰壹拾陆元肆角叁分）。

2、付款方式

合同签订后，乙方向甲方提供合同总价款40%的预付款保函，保函期限至项目验收，甲方在收到乙方发票并确认无误后10日内向乙方支付合同总金额的40%，即人民币¥1060000.00元；乙方完成软件系统开发、系统部署、上线试运行，并向甲方提供合同总价款5%的履约保函，保函期限至服务期结束3个月，甲方验收合格并确认后10日内支付合同总金额的60%，即人民币¥1590000.00元。

3、转账及开票信息

双方确认，甲方通过银行转账方式向乙方以下指定账户支付本合同约定价款。

公司名称：鹤壁豫信电子科技有限公司

纳税人识别号：91410611MA47PY384X

单位地址：鹤壁市淇滨区珠江路与淇水大道交叉口龙门大厦A座三楼

电话号码：0392-3999588

开户银行：中原银行鹤壁分行营业部

银行账户：410601010120000573

甲方将合同款项付至前述账号，即视为甲方已履行付款义务。由于乙方原因造成延迟付款等问题的，一切后果由乙方承担。

开具发票时甲方信息

单位名称：鹤壁市医疗保障局

纳税人识别号：11410600MB1961364M

单位地址：鹤壁市淇滨区黄河路366号

电话号码：0392-3365366

开户银行：中国工商银行股份有限公司鹤壁淇滨支行

银行账号：1710020909200158756

四、双方的权利与义务

1、甲方权利与义务

(1) 甲方有权根据工作需要及时调整产品功能清单，乙方不再另行收费。

(2) 配合乙方及相关单位，进行现状调研、过程管控、技术审查、质量监督、风险控制、交工审查、文档管理、竣工验收等方面的工作。

(3) 为项目建设提供开发测试用机及网络连接等方面的支持，并确保提供的硬软件外部条件符合系统运行的要求。

(4) 及时协调和解决项目进展中因甲方原因出现的问题，使项目能够按期完成。

2、乙方权利与义务

(1) 乙方提供该项目的质量保证服务和技术支持服务。

(2) 乙方项目相关人员在项目建设期间，须认真履行工作职责，努力完成甲方安排的本项目工作任务。

(3) 乙方项目相关人员，负责配合甲方相关部门完成本项目的进行现状调研、过程管控、技术审查、质量监督、风险控制、交工审查、文档管理、竣工验收等方面的工作，并指定项目负责人，与甲方项目负责人一起全权负责项目管理和协调项目中出现的问题，管理项目进度、需求变更、协调本方资源等多方面的工
作。

五、系统验收

1、乙方完成系统部署后，系统进行上线试运行，由乙方书面提出验收申请，甲方应在五个工作日内组织完成项目验收工作，经甲方确认验收通过后，甲方向乙方出具项目验收合格报告。

2、项目验收前乙方应对验收文件进行整理、归集，作为甲方验收的依据，验收文件应随产品一起交付给甲方。

六、产权

1、乙方应保证所提供的全部软件产品、服务或其任何一部分均不会侵犯任何第三方的知识产权，若发生侵权，由乙方承担所有法律责任并全额赔偿因此给甲方造成的损失。

2、服务期到期后，本项目涉及到的软件著作权、设备产权等归甲方所有，同时乙方须向甲方移交本项目涉及的所有定制软件（或定向研发软件）的源代码。

七、保密义务

双方同意，对在合作过程中，任何一方可以获得与本项目有关的对方的商业秘密，对此双方皆应谨慎的进行披露和接受。获取对方商业秘密的一方仅可将该商业秘密用于履行本合同项下的义务，且只能由相关的项目管理和技术实施人员使用，并应采取适当有效的方式保护所获得的商业秘密，不得未经授权使用、传播或公开该商业秘密。保密义务在合同终止后继续有效。

八、服务期及售后服务

1、服务期3年（免费），从验收合格之日起计算。

2、售后服务内容包括软件缺陷、故障及软件功能的部分修改和完善等，用户因完善本项目功能性和性能型需求，对项目部分功能作改动时，乙方应免费给予完成。

3、合同期内，根据工作需要，另行开发模型乙方不得再收取费用。

4、合同期满后的后续服务为有偿服务，相关费用由甲乙双方协商，可另行签订合同进行约定。

九、违约责任

1、本合同任何一方不履行合同或履行合同义务不符合约定条件，即构成违约，另一方有权要求违约方履行或者采取补救措施，并有权要求赔偿损失。一方同意给予对方履行宽限期的，则该宽限期内不应追究另一方违约责任。

2、合同履行过程中，乙方因自身因素导致未按照本合同要求完成项目交付的，每迟延一日，乙方须按合同总额的千分之一向甲方支付违约金，违约金累计不超过合同总额的20%。

十、不可抗力

在本合同执行过程中，由于发生战争、洪水、台风、地震、疫症或其他人力不能控制等不可抗力事件，致使本合同的任何一方无法履行本合同规定的义务，遭受不可抗力的一方不承担违约责任。

遭受不可抗力的一方应在不可抗力事件发生的15天内，向本合同对方出具有关权威部门的证明，并书面说明不可抗力的详细情况，以及合同不能履行，或部分不能履行，或需要延期履行的理由。

受不可抗力影响的一方，应尽可能采取合理的行为和适当的措施减轻不可抗力对本合同履行所造成的影响。没有采取适当措施致使损失扩大的，该方不得就扩大损失的部分要求免责或赔偿。

十一、合同变更与终止

1、合同变更：项目需求确认后，任何一方提出的需求变更，须向对方提供需求变更报告，对方应于3个工作日内做出同意与否的书面回复。若同意变更，双方应于5个工作日内对变更需求进行分析、评估，共同确认由此带来的软件的系统性能、项目技术参数的影响变化以及工作量变化、工期影响等各项事宜，并形成书面补充协议，经双方签字盖章后与本合同具有同等法律效力。

2、合同终止：本合同在双方已履行全部义务时自然终止。

本合同终止后，双方关于知识产权、保密义务、违约责任、特别声明、管辖及争议解决的相关约定仍然有效。

十二、管辖及争议的解决

本合同的解释、效力、履行及其他事宜，均受中华人民共和国法律、法规的管辖。

如双方因履行本合同发生任何争议，应首先协商解决；协商不成，任何一方均可向乙方所在地有管辖权的签约地人民法院提起诉讼。

本合同前述甲、乙双方的地址、电话、邮箱均为双方认可的有效送达地址。上述送达地址适用于通知、协议、法律文书，甲乙双方同意用于人民法院调解、审判及执行程序。邮寄送达被退回的，则以退回之日视为有效送达之日。

上述送达地址、联系人、联系电话等若有变动，一方应在变更前三天内以书面形式通知另一方。若因本合同上注明的地址及联系方式等不准确或变更前未通知对方而导致通知不能送达的，视为一方已送达，另一方承担因此产生的一切后果和责任，同时视为一方已履行通知义务。

双方确认，本合同中约定的上述送达地址适用范围包括双方非诉时各类通知、协议等文件以及就本合同发生纠纷时相关文件和法律文书的送达，同时包括在争议进入仲裁、民事诉讼程序后的一审、二审、再审和执行等程序。

十三、合同生效及其他

本合同自双方的法定代表人或其授权代表签字（或签名章）并加盖各自公章（或合同章）之日起生效。

本合同一式肆份，双方各执贰份，具有同等法律效力。

附件：产品功能清单及分项报价

（以下无正文）

甲方：鹤壁市医疗保障局

法定代表人或授权代表：

签字日期：



陈立峰 2024. 29/9

乙方：鹤壁豫信电子科技有限公司

法定代表人或授权代表：

签字日期：2024. 9. 29



陈鑫印 4106030116049

附件：产品功能清单及分项报价

单位：万元

序号	一级功能	二级功能	技术参数（功能描述）	品牌型号	单位	数量	单价	金额	税率
一、定制化软件开发服务									
1.1 反欺诈数据专区									
1	数据源管理	内部数据源管理	可实现对医保内部反欺诈所需的各类数据源的接入进行增删改配置及查询管理。包括医保数据中台、业务中台、子系统生产库等。	豫信电科定制	项	1	1	1	6%
		外部数据源管理	▲对医保外部反欺诈所需的各类数据源的接入进行增删改配置及查询管理。包括公安、人社、民政、食药监等。						
		离线数据管理	可实现对反欺诈所需的离线数据进行导入和查询管理。						
2	采集任务管理	采集任务管理	可实现根据数据源的配置定义采集任务，包括源地址、源表、源字段和目标地址的定时任务配置。	豫信电科定制	项	1	1	1	6%
		资源分类管理	可实现对采集到的数据表进行分类管理，如可根据业务分类可根据主题分类，可根据数据来源分类等；可查看表结构，可根据表名进行检索。						
3	数据开发	数据开发	▲可实现自行通过 pip line 进行数据开发并形成中间表，生成的中间表亦可纳入到资源分类管理。	豫信电科定制	项	1	5.6	5.6	6%
1.2 医保反欺诈大数据模型									
1	算子管理	数据集算子	可实现包括数据集加载算子和多数据集加载算子的内嵌。	豫信电科定制	项	1	12.4	12.4	6%
		数据处理算子	可实现包括数据切分算子、数据上采样算子、数据下采样算子、特征列选择算子等算子的内嵌。						
		机器学习算子	可实现包括分类、回归、聚类算子的内嵌。						
		自然语言处理算子	可实现包括 jieba 分词算子、CKE中文关键字提取算子、BERT文本分类算子等算子的内嵌。						
		模型评估算子	可实现包括机器学习评估算子和自然语言处理模型评估算子的内嵌。						
2	模型训练	模型训练	可实现通过托拉拽原子算子，形成 pip line 机器学习模型。	豫信电科定制	项	1	8.6	8.6	6%
		模型预测	可实现对机器学习类模型利用测试集进行预测。						
3	模型开发	数据加载	可实现支持对数据资源目录中的各类数据表进行加载	豫信电科定制	项	1	11.8	11.8	6%
		数据关联	可实现支持表关联、字段条件设置和输出列设置						
		数据保存	可实现支持对数据的数据表进行保存，更多用于大数据监测类模型的线索输出。						
4	模型管理	模型管理	可实现对已经发布的模型进行上下线等管理操作；审批和发布操作。	豫信电科定制	项	1	4.8	4.8	6%
		模型评估报告	可实现从模型的描述、审批过程、上线时间、调用次数、产生的绩效(数量和金额 2 个方面) 多个维度进行模型档案全生命周期管理。						
5	模型构建	全场景-高频就诊模型构建	▲模型可实现用于筛查月度或年度内就诊次数极端异常、就诊疾病与机构无明显规律、多次就诊前后缺失一致性的患者记录。模型使用异常检测算法。模型基于就诊记录、结算数据，筛选年度、季度、月度高频就诊人群、综合高频就诊人群，要求高频就诊人在 99%分位数，针对以上人群数据做聚类分析，得到可疑高频就诊参保人。排除特殊人群，如严重慢性病患者、离休干部等人群，以提高高频就诊模型精准度。支持模型的参数配置，模型主要适用于购药、门诊和住院场景。用户可以根据医保区划、模型分析年度月度等条件，查看高频诊断、高频项目、高频参保人信息，并可下钻查看参保人就诊详情，包括参保人姓名、出生日期、性别、机构名称、机构科室、机构医师、诊断、就诊时间、结算项目、结算费用等。	豫信电科定制	项	1	4	4	6%

全场景-进销存(采购)数据模型构建	▲模型主要可实现针对医药机构中药品库存存在异常情况进行筛查分析。模型采用异常检测算法,通过分析药品入库、出库(含调拨、领用、报损、盘点、销售使用等),实时库存等数据,核查异常情况。对医药机构医保药品的采购、销售和库存情况进行监测和管理,确保药品的合理采购、合理销售和合理库存,防止滥用、浪费和虚假报销。	4.3	4.3	6%
全场景-异常收费监测模型构建	该模型可实现主要定位筛查医疗机构执行医疗服务项目收费标准是否存在异常情况,包括是否是超标准收费、超限制用药等。	4.3	4.3	6%
全场景-过度诊疗模型构建	▲模型可实现针对住院患者,对虚构医药服务项目、过度诊疗和过度检查进行筛查。用户可以根据统筹区、医疗机构、时间段等条件,查看风险组情况,并可下钻查看组内参保人信息、机构信息及就诊详情等。	5.8	5.8	6%
住院场景-虚假住院(多人频繁集中住院)模型构建	模型可实现针对相同群体在一段时间内多次同时结伴出入院,根据群组特征分为同机构住院、跨机构住院、同家庭住院。模型采用图算法,以就诊结算、参保人员、单位信息、行为间隔天数、就诊次数的维度形成构图,将结构化数据以图的方式进行重构,将整体切分到区块,使区块内更聚集、区块之间更分明。	5.8	5.8	6%
住院场景-体检住院模型构建	▲可实现体检住院模型挖掘医疗机构低价体检方式诱导无住院需求的参保人入院住院,从而套取医保统筹基金。模型使用线性回归法,用历史数据计算出围绕诊断相关指标的区间值,如住院天数合理上下限,构建诊断与检查项目之间的概率矩阵,判断检查项目使用的合理性,合并挖掘风险。支持模型的参数配置,模型主要适用于住院。	4.2	4.2	6%
住院场景-分解住院模型构建	可实现短时间内(1个月内)因同一种疾病或相同症状再次办理入院的参保人员清单和医疗机构(含科室)清单。	4	4	6%
住院场景-资源消耗异常模型构建	可实现通过引入先进的数据挖掘,可以对海量的医保数据进行深度分析,自动发现异常数据表征。这些算法能够对数据进行模式识别、关联分析、趋势预测等操作从而准确地识别出欺诈行为的蛛丝马迹。	5.6	5.6	6%
住院场景-挂床住院模型构建	可实现筛查同一医疗机构、同一科室、同一床位、同一周期内存在多人就诊的诊疗数据清单。	4.6	4.6	6%
DIP场景-低标住院模型	筛查次均住院费用明显低于该病种平均费用的参保人员清单和医疗机构(含科室)清单。	3.8	3.8	6%
DIP场景-DIP病组高套监管构建	▲建立病组与资源消耗之间的关系,通过整理的诊断或手术关联的核心资源消耗,判断相关病例的资源消耗与病组之间的相关性。	3.8	3.8	6%
门诊药店场景-卡聚集模型构建	▲模型可实现针对大量医保卡非法聚集到某些特定人员手中,并进行统一刷卡套取医保费用,或套取个人账户余额行为的挖掘。模型采用图算法,以参保人、刷卡时间、刷卡地点三个维度形成构图,将结构化数据以图的方式进行重构,将整体切分到区块,使区块内更聚集、区块之间更分明,从而挖掘出不同的团伙。	3.8	3.8	6%
门诊药店场景-购药异常模型构建	模型可实现挖掘药贩或药店自身工作人员收集多张医保卡,并在药店集中刷卡套取医保个人账户资金的违规行为。模型分为集中购药和夜间购药场景。模型采用异常检测算法,单位小时内,刷卡量超高,且时间框架内的同环比挂号数量、挂号人数、总金额、刷卡次数等指标综合考量,划定风险范围。除以上基础数据外,夜间购药还考虑划卡时间非常规程度等因素支持模型的参数配置。	3.6	3.6	6%
其他场景-异地	可实现针对某医疗机构,分病种或全病种监测门诊慢性病异地就医结算费用异常增长情况,且异地的次均费用远高	3.5	3.5	6%

		就医模型构建	于本地次均费用的情况；同时对省内多异地就诊不同病参保人员进行数据监测。							
1.3 监测中心										
1	反欺诈监测中心	人员死亡数据监测	可实现接入公安、民政等第三方数据，按月对医保的死亡人员进行筛查	豫信电科定制	项	1	11.8	11.8	6%	
		住院运营数据监测	可实现针对周期内住院次数与住院人数比、30天再入院监测、低倍率、高倍率等进行数据筛查。							
		门诊/药店购药数据监测	可实现针对频繁门诊/药店购药、高频特药购药进行常规数据筛查；就部分患者门诊或药店购药超过1000元的不合理购药进行数据筛查。							
		药品集采价格监测	可实现针对医疗机构的集采的执行情况进行数据筛查，包括相关同一通用名的药品超过规定的比例、医院采购的药品是否超过集中采购价格等异常数据进行筛查							
2	异常数据疑点线索反欺诈稽核中心	疑点监测	异常数据疑点线索稽核中心是对反欺诈大数据模型的违规数据捕获，通过对监测中心和大数据模型分析的疑点数据进行集中展示，基金监管人员进一步对异常信息进行分析研判，深度放大异常线索追踪链路。按属地管理原则分办、转办，将疑点数据线索分别推送至市级稽核办案机构、县区医保部门的稽核人员开展现场监督检查；核查结论在规定时限内，统一录入反馈至系统平台，形成线上线下一体化稽核闭环体系。	豫信电科定制	项	1	4.6	4.6	6%	
3	反欺诈实时曝光警示中心	曝光警示	打造医保反欺诈实时曝光警示平台，在部分重点公立定点医院机构统一部署宣传屏幕、展板等宣传媒介，充分发挥定点医院机构医保反欺诈宣传主阵地优势，实时曝光、播放欺诈骗保案件，以案释法。	豫信电科定制	项	1	4.6	4.6	6%	
1.4 反欺诈智慧驾驶舱										
1	反欺诈智慧驾驶舱	全局风险画像	可实现按照全局、分区县、分医疗机构、分业务场景等，以数字概要、标签、曲线、柱形、圆形等多种形式，全方位展示当前主题内医保反欺诈大数据应用总体情况，为精准高效决策提供数智支撑。	豫信电科定制	项		4.2	4.2	6%	
2	统一门户集成	/	可实现就整体框架、菜单、用户、权限等信息在统一门户进行集成。	豫信电科定制	项	1	3.5	3.5	6%	
1.5 网络环境搭建										
1	骨干网一期网络链路租赁费用	/	骨干网一期网络链路租赁费用的投入，用于建立高效、稳定的网络链路。可实现为医保数据的传输和共享提供有力保障，确保各部门之间能够快速、准确地交流信息，从而更好地协同开展反欺诈工作。	豫信电科定制	年	1	29.2	29.2	6%	
2	骨干网二期网络链路租赁费用	/	骨干网二期网络链路租赁费用则进一步强化和扩展了网络链路。可增加网络覆盖范围和带宽，以应对日益增长的数据量和业务需求。有助于更全面地监控医保业务，及时发现异常情况。	豫信电科定制	年	1	12.8	12.8	6%	
3	骨干网络安全提升项目	下一代防火墙（部署于市医保局办公网）	硬件架构参数：采用非X86多核架构，1U机架式设备，8个千兆电口+2对Combo口（含1个管理电口）+2个Bypass口，1个Console口，2个USB口，电源：单交流电源，可扩展硬盘插：1个，含1块1T HDD SATA硬盘 性能参数：三层吞吐量4Gbps，七层吞吐量2Gbps，并发连接数100万，每秒新建连接数（HTTP）2.2万 威胁吞吐：IPS吞吐600M，AV吞吐600M，全威胁吞吐400M，SSL VPN最大并发用户数（需单独购买）100，SSL VPN吞吐量40M，IPSEC隧道数量100，IPSEC最大加密性能45M 默认配置授权：含三个月入侵防御、防病毒、应用识别、URL过滤，威胁情报、Web防护试用特征库，15个SSL VPN	H3C SecPath F100-0-AK1015	台	1	7	7	13%	

		<p>用户授权，链路负载不限制链路数量</p> <p>安全托管服务:含一年安全托管基础版服务，支持对设备进行统一纳管与策略下发，实时监测设备运行状态，支持自定义设备告警规则，在生成告警的第一时间以邮件形式对用户或运维工程师进行通报，支持按月推送安全分析报告</p> <p>功能:支持路由、透明、混合模式部署，支持U盘零配置上线，支持基于AI的策略冗余分析、策略命中分析以及应用风险调优等能力，支持资产扫描、加密流量检测、应用审计、数据安全、网页过滤、带宽管理、IPS、AV、WAF等应用层安全功能，支持链路负载、服务器负载，支持SSLVPN、IPSECVPN等多种VPN功能，支持国密算法，支持IPV6协议，支持网页诊断功能，支持多虚一集群以及一虚多虚拟化功能等</p> <p>▲支持IPsec VPN智能选路，根据隧道质量调度流量。</p> <p>▲支持联动云端URL地址库进行全面实施核查。</p>						
	<p>网络入侵防御系统 (市区骨干网)</p>	<p>硬件架构参数:采用非X86多核架构，2U机架式设备，14个千兆电口+12个千兆光口+4个万兆光口，1个Console口，2个USB口，电源:冗余电源，可扩展槽位:4个，可扩展硬盘插:2个，支持双硬盘Raid，含1块1T HDD SATA硬盘，1块250W交流电源</p> <p>性能参数:三层吞吐量18Gbps，七层吞吐量6Gbps，并发连接数450万，每秒新建连接数(HTTP)10万</p> <p>威胁吞吐:IPS吞吐5G，AV吞吐5G，全威胁吞吐2.8G，SSL VPN最大并发用户数(需单独购买)6000，SSL VPN吞吐量600M，IPSEC隧道数量4000，IPSEC最大加密性能2G</p> <p>默认配置授权:含三个月入侵防御，防病毒、应用识别、URL过滤、威胁情报试用特征库，15个SSL VPN用户授权，链路负载不限制链路数。</p> <p>安全托管服务:含一年安全托管基础版服务，支持对设备进行统一纳管与策略下发，实时监测设备运行状态，支持自定义设备告警规则，在生成告警的第一时间以邮件形式对用户或运维工程师进行通报，支持按月推送安全分析报告。</p> <p>功能:支持路由、透明、混合模式部署，支持U盘零配置上线，支持基于AI的策略冗余分析、策略命中分析以及应用风险调优等能力，支持资产扫描、加密流量检测、应用审计、数据安全、网页过滤、带宽管理、IPS、AV、WAF等应用层安全功能，支持链路负载、服务器负载，支持SSL VPN、IPSEC VPN等多种VPN功能，支持国密算法，支持IPV6协议，支持网页诊断功能，支持多虚一集群以及一虚多虚拟化功能等</p> <p>▲支持基于对包括但不限于操作系统、网络设备、办公软件、网页服务等保护对象的入侵防御策略，支持基于对漏洞、恶意文件、信息收集类攻击等的攻击分类的防护策略，支持基于服务器、客户端的防护策略。且缺省动作支持黑名单</p> <p>▲支持报文示踪功能，支持真实流量、导入报文、构造报文等方式，用于分析和追踪设备中各个安全业务模块(如:攻击防范、uRPF、会话管理和连接数限制等)对报文的处理过程，通过查看报文示踪记录的详细信息，有利于管理员对网络故障的快速排查和定位。</p>	<p>H3C SecPath F1000- AK1215</p>	<p>台</p>	<p>1</p>	<p>12</p>	<p>12</p>	<p>13%</p>

		<p>网络入侵防御系统（县接入区）</p> <p>硬件架构参数:采用非X86多核架构, 1U机架式设备, 8个千兆电口+2对Combo口(含1个管理电口)+2个Bypass口, 1个Console口, 2个USB口, 电源:单交流电源, 可扩展硬盘插槽:1个, 含1块IT HDD SATA硬盘</p> <p>性能参数:三层吞吐量4Gbps, 七层吞吐量2Gbps, 并发连接数100万, 每秒新建连接数(HTTP)2.2万</p> <p>威胁吞吐:IPS吞吐600M, AV吞吐600M, 全威胁吞吐400M, SSL VPN最大并发用户数(需单独购买)100, SSL VPN吞吐量40M, IPSEC隧道数量100, IPSEC最大加密性能45M。</p> <p>默认配置授权:含三个月入侵防御、防病毒、应用识别、URL过滤、威胁情报、Web防护试用特征库, 15个SSL VPN用户授权, 链路负载不限制链路数量。</p> <p>安全托管服务:含一年安全托管基础版服务, 支持对设备进行统一纳管与策略下发, 实时监测设备运行状态, 支持自定义设备告警规则, 在生成告警的第一时间以邮件形式对用户或运维工程师进行通报, 支持按月推送安全分析报告。</p> <p>功能:支持路由、透明、混合模式部署, 支持U盘零配置上线, 支持基于AI的策略冗余分析、策略命中分析以及应用风险调优等能力, 支持资产扫描、加密流量检测、应用审计、数据安全、网页过滤、带宽管理、IPS、AV、WAF等应用层安全功能, 支持链路负载、服务器负载, 支持SSL VPN、IPSEC VPN等多种VPN功能, 支持国密算法, 支持IPV6协议, 支持网页诊断功能, 支持多虚一集群以及一虚多虚拟化功能等</p> <p>▲支持BFD和NQA网络协议, 支持基于接口状态和路由状态等多种类型的探测机制来及时触发链路切换或主备切换, 保障业务连续性。</p> <p>▲支持对检测到的攻击行为的前后报文进行自动化抓包功能, 方便用户对攻击行为进行取证</p>	H3C SecPath F1000-AK1015	台	1	7	7	13%
		<p>等保一体机</p> <p>部署于市医保骨干网络运维区, 提供64个日志审计授权, 50个堡垒机运维授权, 128个IP漏扫授权</p> <p>硬件参数:采用通用X86服务器, 规格:2U; 接口:4千兆电; 电源:冗余电源; 硬盘:4T; 内存:96G。</p> <p>性能参数:日志审计处理能力:4000条/秒; 运维审计图形并发/字符并发:150/300; 漏洞扫描最大并发扫描IP数:60; 数据库审计SQL处理能力:15000条/秒; 终端杀毒支持agent数量:0~100个。</p> <p>默认授权:无, 各功能组件以实际选择为准, 支持5选4及以下。</p> <p>功能简述:采用旁路部署模式, 不改变网络拓扑结构, 具备日志审计、漏洞扫描、运维审计、数据库审计、终端杀毒功能, 可在管理平台进行各个组件的基础安全业务策略配置, 对各个组件的运维数据进行集中统计展示。</p> <p>▲支持用户自定义统计维度展示关联事件审计结果, 最多同时展示6个维度审计结果</p>	H3C SecCenter X6015	台	1	35	35	13%
1.6 政务云系统安全要求								
1	云服务器安全防护	采用虚拟防火墙、漏洞扫描、租户隔离、加密保护、安全认证等服务（由政务云服务商提供或协助）。	豫信电科定制	项	1	6	6	13%
2	数据安全防护	<p>数据资源安全防护, 加强数据安全技术管控。进行数据分类分级管理, 采取数据加密、数据脱敏、数据审计等技术措施, 严格管控数据访问行为, 防止数据失密泄密。</p> <p>数据分类分级管理: 实施严格的数据分类分级策略, 根据数据的敏感度、重要性及潜在风险, 对数据进行精细化分类与定级。</p> <p>数据加密保护: 采用先进的加密技术, 对敏感数据进行加密存储和加密传输。确保数据在存储介质中和网络传输过程中均处于加密状态, 即使数据被非法获取, 也无法轻易解密, 从而有效防止数据泄露和未授权访问。</p> <p>数据脱敏处理: 对于需要在非安全环境下共享或测试的数</p>	豫信电科定制	项	1	7	7	13%

			据，实施数据脱敏处理。通过替换、掩码或删除敏感信息的方式，降低数据的敏感度，满足合规性要求。 数据访问控制：基于最小权限原则，实施精细化的数据访问控制策略。明确每个用户或角色的数据访问权限，并通过身份认证、访问授权和访问审计等机制，确保只有经过合法授权的用户才能访问其权限范围内的数据，严格限制数据的访问范围和使用方式，防止数据失密泄密。						
3	系统安全评测服务	/	定期开展渗透测试，常态化开展基线检查、漏洞扫描，主动发现安全漏洞并及时修改，年度等保测评与密码安全性评估。	豫信电科定制	项	1	3	3	6%
4	终端安全服务	/	系统有关的终端设备安装终端安全管理程序，具备防病毒、资产管理、漏洞管理、外设管控、进程管控、网络准入、零信任准入等功能。	豫信电科定制	项	1	7	7	6%
5	安全日志对接	/	系统所有安全设备、服务器、中间件、数据库、应用系统等开展常态化日志采集，实现与市安全运营支撑平台对接。	豫信电科定制	项	1	4	4	13%

