河南省医疗保障局河南省医疗保障业务骨干网络运行维护项目（B包）技术服务合同

甲方（委托方）：河南省医疗保障局；

住　所　地：河南省郑州市郑东新区正光路11号；

法定代表人：/；

项目联系人：董老师；

联系方式：0371-69698572；

通讯地址：河南省郑州市郑东新区正光路11号；

电　　话：0371-69698572 传　　真：0371-69698572

电子信箱：hnyxsanbu@163.com

乙方（受托方）：联通(河南)产业互联网有限公司；

住　所　地：郑州市中原区华山路105号芝麻街E区8栋；

法定代表人：王晓明；

项目联系人：王云泽；

联系方式：18639552296；

通讯地址：郑州市中原区华山路105号芝麻街E区8栋；

电　　话：18639552296 传　　真：/；

电子信箱：niuly1@chinaunicom.cn；

鉴于：甲方委托河南豫信招标有限责任公司通过竞争性磋商方式对河南省医疗保障局河南省医疗保障业务骨干网络运行维护项目（B包）（项目编号：豫政采(2)20252240-2）进行公开采购，经磋商小组评定，乙方为该项目的成交供应商。

本合同甲方委托乙方就 河南省医疗保障局河南省医疗保障业务骨干网络运行维护项目（B包） 进行的专项技术服务，并支付相应的技术服务报酬。双方经过平等协商，在真实、充分地表述各自意愿的基础上，根据《中华人民共和国民法典》的相关规定，达成如下协议，并由双方共同恪守。

第一条 技术服务内容

1. 技术服务的具体内容和总体目标是： 通过采购科学、标准、专业、安全的第三方技术支持服务，实现系统运维的规范化、制度化、流程化管理，不断优化运行环境和系统性能，解决各种运行保障和业务需求，保障系统安全、稳定、高效运行，提高办公效率和质量，提升政务系统的决策能力和应急能力。

2. 为了切实做好系统的运行维护工作，开展技术服务应遵循以下总体工作原则：保密原则、安全原则、属地化管理原则、可控性原则、最小影响原则。

3. 维护的业务系统范围为：省医保骨干网所有软硬件设备的运维及原厂质保服务，包含：产品系统升级授权、远程支持服务、产品保修服务、硬件故障上门支持、提供一年原厂售后服务承诺函。

4. 技术服务内容：采购文件、答疑纪要（如有）以及变更通知（如有）范围内的全部内容，包括但不限于：（1）网络及安全设备运维服务；（2）日常运维服务，具体详见附件《技术规范书》。

第二条 技术服务要求

乙方应按下列要求完成技术服务工作：

1. 技术服务地点：甲方指定地点；

2. 技术服务期限：2026 年 1 月 1 日至 2026 年 12 月 31 日。；

3. 技术服务质量要求：乙方的服务应符合本合同约定的服务要求和技术规范；

4.禁止转包：未经甲方书面同意，乙方不得将本合同项下的服务分包给任

何第三方；

5. 其它约定事项：

（1）乙方派遣人员必须严格遵守甲方的相关工作管理制度，并按照要求签订保密协议和个人保密承诺书；乙方按照国家相关法律规定，全权负责派遣人员的工资、福利、食宿、交通、人身安全、心理健康等事项，合同履行期间派遣人员的上述事项甲方概不负责；

（2）乙方必须严格按照要求派遣相应人员，受甲方管理，必须遵守甲方的制定的《驻场人员管理办法》等管理制度，并按照甲方要求开展工作，派遣人员不符合甲方工作要求，出现：工作进度缓慢，技术支持服务不符合要求，不遵守工作纪律，不服从甲方系统管理员要求等情形的，甲方有权更换相关派遣人员并要求乙方开展相应的整改工作。甲方可视情节严重情况，从质量保证金中扣除相应费用作为惩戒。

（3）若乙方提供的技术支持和服务不全面而导致系统功能无法实现或不能完全实现，由乙方无偿进行补足、完善，造成损失的一并承担赔偿责任。在项目实施中，乙方需要对系统设计进行必要的变更，或者使用特定的硬件和软件，应提出变更说明，并在征求甲方同意后，负责重新设计安装。

（4）为了规范和提高本项目服务水平，乙方要加强对技术支持服务工作的总结，配合甲方开展研究工作，并将研究成果在核心期刊上发表。

（5）甲方支付的合同款已包含本项目审核、成果验收等费用。

第三条　协作事项

为保证乙方有效进行技术服务工作，甲方应当向乙方提供下列工作条件和协作事项：

1. 提供技术资料：

（1）合同内应用系统需要安装第三方软件的安装文件、使用说明、安装说明；

（2）合同内应用系统服务器的配置、IP 的配置、服务器存放位置信息 ；

（3）省医保骨干网日常维护人员的联系方式。

2. 提供工作条件：

（1）甲方为乙方提供3个工位及相关网络IP、网线等，驻场人员专用电脑由乙方配备；

（2）甲方为乙方提供进行系统配置的相应的系统权限和账号。

第四条 技术服务费用及支付方式

1. 双方确认，技术服务费总额为¥975000.00元(大写：人民币玖拾柒万伍仟元整)，其中，不含税总价款为：¥919811.32元（大写：人民币玖拾壹万玖仟捌佰壹拾壹元叁角贰分）；税金：¥55188.68元（大写：人民币伍万伍仟壹佰捌拾捌元陆角捌分），税率6%。甲方支付的服务费包括乙方为完成本合同项下全部义务所支出的费用，除此之外，甲方不再支付其他任何费用。

2. 技术服务费由甲方 分期 （一次或分期）支付乙方。

具体支付方式和时间如下：

（1） 自合同签订之日起3个月内，甲方向乙方指定账户支付技术服务费总额的40%，即¥390000元（大写：人民币叁拾玖万元整）；

（2） 乙方完成本合同项下全部技术服务工作，经验收合格后15个工作日内，甲方向乙方支付技术服务费总额的60%，即¥585000元（大写：人民币伍拾捌拾万伍仟元整）。

3. 支付流程

（1）本合同的每笔资金支付前，乙方应先向甲方提交书面支付申请，支付申请书应写明支付金额、支付依据，并附带符合甲方财务要求与支付金额等值的发票。

（2）本合同约定的付款期限为财政资金支付的一般期限，如因财政支付流程原因导致的支付迟延，不视为甲方违约，但甲方应协助乙方尽快完成财政支付流程。

4.乙方同意甲方将该款项支付至乙方指定的如下银行账户：

乙方开户银行名称、地址和帐号为：

开户银行：招商银行郑州分行营业部

地址：河南自贸实验区郑州片区（郑东）农业东路96号

帐号：371906633710688

社会信用代码：11410000MB16715277

5.如上述银行账户发生变更，乙方应当在甲方每次付款前书面通知乙方，因乙方变更银行账户通知不及时造成的损失，由乙方自行承担。

第五条　保密义务

甲方的保密义务：

1. 保密内容（包括技术信息和经营信息）：涉及乙方技术秘密的资料、信息、数据和其它秘密事项。

2. 涉密人员范围：参与本项目的所有技术人员、领导、专家。

3. 保密期限：长期。

4. 涉密责任：赔偿乙方由此造成的损失，并承担法律责任。

乙方的保密义务：

1. 保密内容（包括技术信息和经营信息）：涉及国家秘密、甲方技术秘密和甲方明确不能公开的资料、信息、数据和其它秘密事项。

2. 涉密人员范围：参与本项目的所有技术人员、领导、专家。

3. 保密期限：长期。

4. 涉密责任：赔偿甲方由此造成的损失，并承担法律责任。

第六条　合同变更

本合同的变更必须由双方协商一致，并以书面形式确定。

第七条 项目验收

双方确定，按下列标准和方式对乙方提交的技术服务工作成果进行验收：

1. 乙方提交技术服务成果的形式及时间：文档，月报于次月中旬前提交，季报于次月中旬前提交，年报按甲方要求时间提交。

2. 技术服务工作成果的验收标准：技术服务规范；维护文档齐全；未发生大的故障；服务需求得到及时响应、服务质量符合要求，并按甲方要求，在核心期刊发表一篇关于本项目的论文。

3. 技术服务工作成果的验收方法：日常考勤考核，听取技术服务报告，对报告进行核查。

4. 验收的时间和地点：维护期结束前 1 个月内，甲方指定地点。

5. 验收提交成果：月报、季报、每季度巡查报告、每半年安全检测报告、年度总结报告、系统管理员知识库等。

第八条　成果权利归属

1. 在本合同有效期内，甲方利用乙方提供的技术服务工作成果所完成的新的技术成果，归甲方所有。

2. 在本合同有效期内，乙方利用甲方提供的技术资料和工作条件所完成的新的技术成果，归甲方所有。

第九条　违约责任

1.甲乙双方均应全面、诚信履行本合同约定的各项权利义务。因一方违反本合同约定的，应依法承担违约责任，并赔偿对方因此遭受的损失。

2.乙方有下列情形之一的，甲方有权解除本合同，乙方除返还甲方已支付未履行期间的技术服务费用外,还应当按照技术服务费用总额 10%的标准向甲方支付违约金，并赔偿甲方因此遭受的全部损失（包括但不限于：甲方另行委托其他人完成该项目的费用、甲方支付的诉讼费用及律师费用）。

（1）乙方未依照合同约定的时间、内容、标准完成工作，经甲方催告后，乙方在合理期限内仍未完成的。

（2）乙方降低或不执行技术服务质量要求，不具备完成项目所需的条件和能力，在服务中有弄虚作假和重大欺骗行为的。

（3）在甲方指定的整改期限内，乙方拒不整改或整改后仍不能满足质量要求的。

（4）乙方及其雇员违反本合同约定的保密义务的。

（5）乙方提供的成果侵犯第三方知识产权的。

（6）未经甲方书面同意，乙方擅自将本合同工作转包或分包给其他单位或个人的。

3.合同解除后，如需继续完成该服务项目，甲方有权另行选择第三方，并无偿使用乙方已完成的工作及其成果。甲方继续使用的行为不免除或减轻乙方应承担的违约责任。

4.乙方应向甲方支付的违约金、损害赔偿金及其他应付款项，甲方有权从应付乙方的技术服务费用中直接抵扣，乙方对此无异议。

第十条　沟通联络

双方确定，在本合同有效期内，甲方指定 董老师 为甲方项目联系人，乙方指定王云泽为乙方项目联系人。项目联系人承担以下责任：

1. 全权配合项目实施及组织协调项目的开展、验收工作；

2. 涉及本项目的其他有关事务。

一方变更项目联系人的，应当及时以书面形式通知另一方。未及时通知并影响本合同履行或造成损失的，应承担相应的责任。

第十一条　合同解除

双方确定，因出现不可抗力或当事人一方因故不能履行合同时，征得对方同意后双方可以解除合同；出现客观情况致使本合同的履行成为不必要或不可能的，亦可以解除本合同。

第十二条　争议解决

双方因履行本合同而发生的争议，应协商解决。协商不成的，同意依法向甲方所在地人民法院起诉。

第十三条 附则

1.与履行本合同有关的相关技术文件，相关技术资料 、附件等为本合同的组成部分，与本合同具有同等法律效力。

2.本合同未尽事宜，双方可另行签订补充协议，补充协议与本协议具有同等法律效力，补充协议与本合同不一致的地方，以补充协议为准。

3.本合同一式 陆 份，甲乙双方各执 叁 份，具有同等法律效力。本合同经双方法定代表人或授权代理人签字盖章后生效。

4.本合同竞争性磋商文件、响应文件、成交确认书等均系本合同不可分割的重要组成部分，与本合同具有同等法律效力。

5.本合同约定的当事人联系方式和地址作为本合同项下各种文书及发生争议时所涉诉讼文书的有效送达地址。任何一方按上述地址进行送达，因无人签收、拒收等原因导致被退回的，退回之日即为送达之日。上述地址发生变更，变更方应在变更前 7 日内书面通知对方，否则按上述地址进行的送达仍然有效。

（以下无正文）

【本页无正文，系《河南省医疗保障局河南省医疗保障业务骨干网络运行维护项目（B包）技术服务合同》签署页】

甲方：河南省医疗保障局（盖章）

法定代表人/委托代理人：（签名）

2026年1月5日

乙方：联通(河南)产业互联网有限公司（盖章）

法定代表人/委托代理人：（签名）

2026年1月5日

附件：技术规范书

一、网络及安全设备运维服务

1、服务期限

本次项目总体服务期限为：2026 年 1 月 1 日至 2026 年 12 月 31 日。

2、服务内容

（1）提供省医保骨干网所有软硬件设备的运维及原厂质保服务，包含：产品系统升级授权、远程支持服务、产品保修服务、硬件故障上门支持、提供一年原厂售后服务承诺函。

（2）提供省医保骨干网所有安全设备的特征库升级服务。

二、日常运维服务

1、服务期限

本次项目总体服务期限为：2026 年 1 月 1 日至 2026 年 12 月 31 日。。

2、服务人员

在合同服务期限内，B 包提供 2 名技术人员组成的驻场服务团队以完成日常运维服务、节假日值守及安全应急事件处置；

技术能力：服务人员具备先进的网络安全技术和工具，包括漏洞扫描工具、入侵检测系统、防火墙、防病毒软件等。能够运用大数据分析、人工智能等技术手段，提高网络安全监测和分析的效率和准确性。

其他要求：服务人员须具备优秀的技术能力、沟通能力和职业素养，服务人员的简历须经过采购人审定同意后方能开展工作。服务人员日常工作由采购人指定，未经同意，投标人不得更换人员。若服务人员不能有效完成采购人工作要求，

自采购人提出更换要求日起3日内投标人需更换人员。

3、主要服务内容

（1）资产梳理

对省医保骨干网络相关的硬件、软件、网络、数据、账号等资源进行全面盘点、识别、分类并建立资产台账。

根据资产梳理内容，绘制网络拓扑，统计信息点分布以及各硬件设备和软件系统的数量、拓扑位置、用途等信息。结合资产梳理，形成资产台账。

（2）网络安全设备软硬件服务

网络和安全设备的硬件日常维护、软件更新、软件升级、特征库升级、设备维护、故障检测及故障处理。

（3）网络安全监测

实时监控：通过专业的网络安全监测工具，对信息化资产进行 7×24 小时实时监控，包括网络流量、系统日志、安全设备状态等。及时发现异常流量、攻击行为、系统漏洞等安全事件，并进行准确记录。

威胁情报收集与分析：持续关注国内外网络安全动态，收集各类威胁情报信息。结合当前网络环境特点，对威胁情报进行深入分析，评估潜在威胁对信息化资产的影响程度，提供针对性的解决方案。

（4）安全漏洞管理

使用专业的漏洞扫描工具，定期对全网进行漏洞扫描服务，按照约定的周期（最低每月一次），对信息化资产（服务器、网络设备、应用系统、医保终端等）进行全面的漏洞扫描。对扫描发现的漏洞进行详细分析，评估漏洞的严重程度、可能造成的影响以及被利用的风险。根据漏洞的评估结果，提供清晰、易懂的漏

洞报告，包括漏洞描述、修复建议和优先级排序。

协助省局及地市制定漏洞修复计划，跟踪漏洞修复进度，确保漏洞得到及时、有效的修复。对于暂时无法修复的漏洞，提供相应的临时防护措施，降低安全风险。

（4）网络安全防护

防火墙策略配置与优化：根据网络架构和业务需求，制定合理的防火墙策略。定期对防火墙策略进行审查和优化，确保防火墙能够有效阻挡外部网络攻击，同时保障内部网络的正常访问。及时更新系统的规则库，提高对新型攻击的检测和防范能力。对系统产生的报警信息进行及时处理和分析，采取相应的措施应对入侵行为。

恶意软件防范：通过防病毒软件、恶意软件检测工具等，对网络中的终端设备、服务器等进行实时防护。定期更新病毒库和恶意软件特征库，确保能够及时发现和清除各类恶意软件。对感染恶意软件的设备进行隔离和处理，防止恶意软件的传播和扩散。

（5）应急响应服务

协助制定完善的网络安全应急响应预案，明确应急响应流程、人员职责和应急处置措施。定期对应急响应预案进行演练和修订，确保预案的有效性和可操作性。

在接到网络安全事件报警后，立即启动应急响应机制。迅速组织专业的应急响应团队，对事件进行调查和分析，确定事件的性质、影响范围和损失程度。采取有效的应急处置措施，如隔离受感染设备、阻断攻击源、恢复数据等，最大限度地降低事件对业务的影响。

在应急响应结束后，及时提交详细的事件报告，包括事件发生的原因、经过、处置措施和结果等。对事件进行深入总结和分析，提出改进建议和预防措施，帮助完善网络安全防护体系。

能够按照故障分级响应机制完成应急处理，故障分级响应机制如下：

故障级别	故障定义	故障描述	解决时间
一级故障	设备在运行中出现系统瘫痪或服务中断，导致设备的基本功能不能实现或全面退化的故障，造成业务中断1小时以上或导致关键业务数据	业务中断1 小时以上;业务数据丢失	恢复≤1小时
二级故障	设备在运行中出现的直接影响服务，导致系统性能或服务部分退化的故障；设备在运行中出现的故障具有潜在的系统瘫痪或服务中断的危险，并可能导致设备的基本功能不能实现或全面退化，如冗余设备单侧故障等；系统设备或操作系统	冗余设备单侧故障	恢复≤2小时
三级故障	设备在运行中出现影响系统功能和性能，但关键业务不受影响的故障。	业务不受故障影响	恢复≤3小时
四级故障	软件功能、安装或配置方面需要信息或支持，对业务运作无影响。	对业务运作无影响	恢复≤4小时

（6）重保支撑

在护网或其他重保期间要求进行现场重保值守。

值守人员具备扎实的网络安全专业知识，熟悉常见的网络攻击类型（如DDoS 攻击、恶意软件入侵、SQL 注入等）及其防范方法。能够熟练运用各类网络安全工具，如防火墙、入侵检测系统、漏洞扫描工具等进行实时监测和分析。

了解网络架构、关键业务系统的运行原理和安全需求。熟悉骨干网络的网络安全策略、应急预案以及相关安全管理制度，确保在遇到问题时能够准确判断并采取正确的应对措施。

具备快速响应和处理网络安全突发事件的能力。在面对紧急情况时保持冷静，能够迅速分析问题的性质和影响范围，按照既定的应急预案采取有效的措施进行处置，最大限度地降低事件对业务的影响。

定期参加网络安全应急演练，提高实际操作能力和团队协作能力。通过演练积累经验，不断优化应急处理流程，确保在实际发生安全事件时能够高效、有序地应对。

（7）定期巡检

全省 18 个地市骨干网络节点核心设备的运行状态巡检（每月≥1 次）及性能调优。

执行每日健康检查、每周性能分析及每月深度巡检（包括配置合规性核查），并提交相应的巡检报告。

防火墙、入侵检测系统（IDS）、堡垒机等安全设备的策略管理、日志审计及漏洞修复。定期开展网络安全风险评估（每季度≥1 次）和漏洞扫描（每月≥1 次）。

每半年提供网络运行分析报告，包含性能瓶颈、优化建议及风险预警。每年组织≥2 次医保系统管理员网络技术培训。

（8）其他要求

编制并更新网络拓扑图、设备清单、应急预案等技术文档。配合完成医保信息系统等级保护测评（等保 2.0）及合规整改。

配合完成医保骨干网络结构优化调整等工作。

4、服务质量保障

响应时间：对于紧急的网络安全事件，应在接到报警后 10 分钟内做出响应，并在 2 小时内到达现场进行处理（如需要现场支持）。对于非紧急的服务请求，应在 1 个工作日内给予回复，并在约定的时间内完成服务。

事件处理成功率：对于各类网络安全事件，确保事件处理成功率达到 95%以上。对未能成功处理的事件，及时说明原因，并提供进一步的解决方案。

漏洞修复率：在漏洞管理服务中，确保网络设备、安全设备的漏洞修复率达到 100%。对于未能及时修复的漏洞，说明原因，并提供相应的风险缓解措施。

三、设备清单

二期设备

1、网络及安全设备					
1.1 省级设备					
1.1.1	上联路由器	华为、NE40E-X8A	台	1	省级骨干路由区
1.1.2	下联路由器	华为、NE40E-X8A	台	1	省级骨干路由区
1.1.3	防火墙	绿盟、NFNX5-HD6300	台	1	横向接入区

1.1.4	LNS 设备	华为、ME60-X8A	台	1	横向接入区
1.1.5	防火墙	绿盟、NFNX5-HD5100	台	1	安全管理区
1.1.6	交换机	华为、S7703	台	1	安全管理区
1.1.7	统一网络管理系统	华为、esight	套	1	安全管理区
1.1.8	网管服务器	华为、2288X V5	台	1	安全管理区
1.1.9	堡垒机	绿盟、OSMSNX3-1000C	台	1	安全管理区
1.1.10	日志审计	绿盟、LASNX3-HD2000	台	1	安全管理区
1.1.11	漏洞扫描	绿盟、RSASNX3-E	台	1	安全管理区
1.1.12	电脑主机杀毒软件	金山、KSV9	套	1	安全管理区
1.1.13	APT 未知威胁	绿盟、TACNX3-D2000A	套	1	安全管理区
1.1.14	态势感知	绿盟、TSOP	套	1	安全管理区
1.1.15	应用负载均衡系统	深信服、AD-1000-B2650-TK（深信服应用交付网关）	台	2	安全管理区
1.1.16	防火墙	绿盟、NFNX3-HD2320	台	2	办公区
1.1.17	核心交换机	锐捷、RG-S7808C	台	2	办公区
1.1.18	接入交换机	锐捷、	台	36	办公区

		RG-S5310-48GT4XS-E			
小计				56	——
1.2 郑州、商丘、驻马店、信阳、洛阳设备					
1.2.1	上下联路由器	华为、NetEngine8000 M14	台	10	骨干路由区
1.2.2	防火墙	绿盟、NFNX5-HD6300	台	4	横向接入区
1.2.3	LNS 设备	华为、ME60-X8A	台	4	横向接入区
1.2.4	防火墙	绿盟、NFNX3-D1200	台	4	办公区
1.2.5	交换机	锐捷、RG-S5310-48GT4XS-E	台	8	办公区
1.2.6	堡垒机	绿盟、OSMSNX3-HD200	台	4	安全管理区
小计				34	——
1.3 新乡、安阳、平顶山、开封、许昌、焦作设备					
1.3.1	上下联路由器	华为、NetEngine8000 M8	台	12	骨干路由区
1.3.2	防火墙	绿盟、NFNX5-HD5100	台	6	横向接入区
1.3.3	LNS 设备	华为、ME NetEngine8000 M14	台	6	横向接入区
1.3.4	防火墙	绿盟、NFNX3-D1200	台	6	办公区
1.3.5	交换机	锐捷、RG-S5310-48GT4XS-E	台	12	办公区

1.3.6	堡垒机	绿盟、OSMSNX3-HD200	台	6	安全管理区
小计				48	——
1.4 漯河、三门峡、鹤壁、济源设备					
1.4.1	上下联路由器	华为、NetEngine8000 M6	台	8	骨干路由区
1.4.2	防火墙	绿盟、NFNX5-HD4100	台	4	横向接入区
1.4.3	LNS 设备	华为、ME NetEngine8000 M14	台	4	横向接入区
1.4.4	防火墙	绿盟、NFNX3-D1200	台	4	办公区
1.4.5	交换机	锐捷、RG-S5310-48GT4XS-E	台	8	办公区
1.4.6	堡垒机	绿盟、OSMSNX3-HD200	台	4	安全管理区
小计				32	——
1.5 省直管县设备					
1.5.1	路由器	华为、NetEngine8000 M6	台	6	骨干路由区
1.5.2	防火墙	绿盟、NFNX5-HD4100	台	6	横向接入区
小计				12	——
1.6 其他县（市、区）设备					
1.6.1	出口防火墙	绿盟、NFNX3-D1200	台	133	办公区

1.6.2	接入交换机	锐　　捷　、 RG-S5300-48GT4XS-E	台	266	办公区
小计				399	——