郑州市中心医院国家创伤区域医疗中心信息化建设项目密码、电子签名设备及项目安全服务合同

甲方：郑州市中心医院

乙方：联通（河南）产业互联网有限公司

根据《中华人民共和国民法典》经甲乙双方协商，就甲方向乙方采购**郑州市中心医院国家创伤区域医疗中心信息化建设项目密码、电子签名设备及项目安全服务**（以下简称本项目）相关事宜达成一致意见，现签订本合同内容如下：

一、项目概况

1.1 项目名称：郑州市中心医院国家创伤区域医疗中心信息化建设项目密码、电子签名设备及项目安全服务

1.2 项目地点：郑州市中心医院（包含但不限于院本部、高新院区、康复医院、豫欣老年病医院、文化宫路院区、马寨医院、北京积水潭医院郑州医院及未来将投入使用的院区）

1.3 建设内容：完成郑州市中心医院国家创伤区域医疗中心信息化建设项目密码、电子签名设备及项目安全服务内容，包括并不限于网络安全等级保护测评、商用密码应用安全性评估、日常网络安全服务以及重要时期网络安全保障值守服务。围绕医院信息系统资产（包括主机、网络、应用及数据等）的建设和运行维护场景，全面落实国家网络安全等级保护和商用密码管理相关制度要求，提升医院整体网络安全防护与保障能力

二、建设标准、技术规范及产品质量

2.1 建设标准

（1）设备质量：所供应设备是全新的、未使用过的，需提供原厂供货证明；

（2）技术先进性：除非合同另行规定，所供应设备全部为最新技术；

（3）安全性：所供应设备均应满足运行的高度可靠性；

（4）自主可控：优先使用自主知识产权的国产技术和产品或兼容国产产品及平台，推进信息化核心领域自主安全可控。

2.2 技术规范

根据附件五《服务承诺书》的具体内容，满足法律法规及相关技术规范要求。

2.3 产品质量

合格，符合国家、行业及地区相关标准规范，满足采购人及相关部门的质量要求。为保证质量，乙方需出具产品质量承诺书，详见附件四《产品质量承诺书》。

三、合同期限及支付

3.1 建设周期

自合同签订之日起，软件系统2年完成交付，硬件3个月完成交付，且完成在服务期内所有工作及善后服务。

3.2 合同价款

本合同总价款共计 2,468,650.00 元（大写：人民币 贰佰肆拾陆万捌仟陆佰伍拾元整）。该合同价款中已包含甲方购买的全部产品费用、培训费用、服务费用、税金及乙方合理利润等一切相关费用。

其中：

设备费共计 778600.00 元（大写：柒拾柒万捌仟陆佰元整），不含税价 689026.55 元（大写：陆拾捌万玖仟零贰拾陆元伍角伍分），税金 89573.45 元（大写：捌万玖仟伍佰柒拾叁元肆角伍分）。税率为【13%】

技术服务费共计 1690050.00 元（大写：壹佰陆拾玖万零伍拾元整），不含税价 1594386.79 元（大写：壹佰伍拾玖万肆仟叁佰捌拾陆元柒角玖分），税金 95663.21 元（大写：玖万伍仟陆佰陆拾叁元贰角壹分）。税率为【6%】

合同履行期间，如果国家税率调整，合同金额不变。

3.3 支付方式

合同签订，乙方提交服务方案经甲方确认后，甲方向乙方支付合同总价款的40%，即人民币：玖拾捌万柒仟肆佰陆拾元整（小写：987,460.00 元）

乙方完成硬件设备到货安装工作，且项目验收合格甲方签署《郑州市中心医院国家创伤区域医疗中心信息化建设项目密码、电子签名设备及项目安全服务初验报告》，甲方向乙方支付合同总价款的 40%，即人民币：玖拾捌万柒仟肆佰陆拾元整（小写：987,460.00 元）

乙方完成本合同约定的全部服务，且取得相应的等级保护证明及完成商用密码应用安全评估备案后，甲方向乙方支付合同总价款的 20%，即人民币 肆拾玖万叁仟柒佰叁拾元整（小写：493,730.00 元）

乙方在申请付款前，应向甲方开具合法、有效、足额的增值税专用发票，甲

方收到发票后再行付款，发票信息应与乙方主体信息一致。

3.4 能源成本费

3.4.1 乙方人员驻场后，由甲方判定是否办理表具安装。办理表具安装的，根据工作场所安装表具单独计量，携带《郑州市中心医院用能承诺书》前往总务科办理表具安装，表具由总务科统一安装；不办理表具安装的，甲方将根据乙方设备和驻场人数的最大量所产生的费用据实结算。按照《郑州市能源收费标准》收取（详见附件七）。

3.4.2 甲方每季度统计核算 1 次用能数据，乙方在每季度结束后次月 15 号前按照实际产生费用核算结果到财务科开票结算。

3.5 乙方账户

单位名称：联通（河南）产业互联网有限公司

开户行：中国银行股份有限公司北京西城支行（联行号：104100004499）

账号：214103201101010001

四、服务内容

4.1 服务内容：对不少于 6 个重要信息系统开展三级网络安全等级保护测评和商用密码应用安全性评估服务；提供日常网络安全服务，配备不少于 1 名专职安全服务工程师（同时具有国家信息安全测评中心颁发的 CISP 系列认证证书及国家信息安全审查与认证中心颁发的 CISAW 系列证书），开展风险评估、渗透测试、安全咨询、应急响应及安全培训等工作；提供重要时期网络安全保障值守服务，在重要保障期间配备不少于 3 名具备攻防演习经验的重保安全工程师（具有国家信息安全测评中心颁发的 CISP 系列认证证书或国家信息安全审查与认证中心颁发的 CISAW 系列证书），实施 7×24 小时现场或远程安全监测与值守，确保医院信息系统安全稳定运行。

详见本合同附件一《服务范围及要求》和附件三《技术参数清单》

乙方应确保提供的服务符合相关法律法规的要求，并达到双方约定的质量标准。

4.2 服务形式

乙方安排人员以现场技术服务形式完成本合同约定的服务内容，

五、验收

5.1 本项目完工并达到验收条件后，乙方须按项目验收有关规定向甲方提交完整验收资料。

5.2 乙方完成合同约定的全部服务内容，提供相关报告或证书作为验收及支付依据。

六、甲方权利与义务

6.1 甲方有权随时向乙方了解项目进度，并要求乙方提供项目相关资料。

6.2 甲方有权对服务情况进行监督、检查、考核，并要求乙方提供相关资料，如未达到服务要求，有权对乙方进行处罚。

6.3 甲方有权按照本合同约定或有关法律规定、政府管理的相关职能规定，对本项目进行监督和检查有权要求乙方按照监督检查情况制定相应措施并加以整改，甲方不因行使该监督和检查权而承担任何责任，也不因此减轻或免除乙方根据本合同约定或相关法律法规规定应承担的任何义务或责任。

6.4 甲方有权在乙方履行合同过程中出现损害或可能损害公共利益、公共安全情形时终止本合同。

6.5 甲方有权根据国家政策或法律法规的变动对服务项目的需求标准和质量要求作出相应变动或取消项目。

6.6 甲方有权将乙方履行合同情况及不符合政府购买服务管理规定情况，向相关部门报告并纳入不良信用记录、年检（报）、评估、执法等监管体系中。

6.7 甲方负责协调本项目各种工作。

6.8 甲方负责协调各相关部门配合乙方实施本项目。

6.9 甲方应按照本合同约定支付合同款项。

6.10 本合同期限内，因甲方需要或者业务需求，乙方在提供服务过程中进行系统软件功能调整开发所产生的技术成果归甲方所有。未经甲方同意，包括乙方在内的任何单位或者个人不得使用该技术成果。

七、乙方权利与义务

7.1 乙方有权自甲方处获得与提供本合同项下服务相关的所有必须的文件、资料。

7.2 乙方应配备具有相应资质、特定经验的工作人员负责项目实施，按照本合同约定的标准、要求和时间完成项目。乙方必须按照投标文件提供的团队成员

名单配备人员，无重大事项不得变更项目组人员，确需调整的，应在项目团队成员配置标准的前提下，向甲方提出变更申请，待批准后方可变更。

7.3 乙方不得以任何理由将本合同项下的服务项目转包给第三方承担（招标文件中有特别约定的除外）。

7.4 乙方应全面履行本项目实施过程中的相关安全管理职责，因乙方未尽到管理职责发生安全事故的，由乙方承担相应的法律责任及经济责任。

7.5 乙方承诺根据本合同提供的服务及相关的软件和技术资料，均已取得有关知识产权的权利人的合法授权，如发生涉及到专利权、著作权、商标权等争议，乙方负责处理并承担由此引起的全部法律及经济责任。

7.6 乙方应接受并配合甲方或甲方组织的对本合同履行情况的监督与检查，对甲方指出的问题，应及时作出合理解释或予以纠正。

7.7 乙方向甲方提供系统应用软件以及其他相关新技术和新业务日常技术咨询服务，在甲方要求时，免费提供与第三方系统的互通性方案和相关的数据格式，并进行相关对接开发，达到院内系统之间的互联互通。

7.8 项目交付后，乙方应无条件返还甲方向其提供的文件、资料并向甲方移交项目资料，并对已知悉的甲方所有资料进行长期保密。

7.9 乙方须严格按照招、投标文件要求实施本项目，并根据甲方项目管理要求进行整改。

7.10 乙方驻场人员工作纪律需满足甲方关于第三方人员的管理要求。

7.11 合同期限内，若系统软件版本更新，乙方应免费为甲方提供系统升级服务。

7.12 乙方须向甲方提供原厂商的软件永久使用许可授权书。

7.13 系统最终验收前乙方须提供公安部认可的网络安全风险测评资质的公司或机构做出的网络安全等级保护测评报告、商用密码应用安全性评估报告。

八、服务要求

8.1 本合同签订后，对于甲方提出的服务要求，乙方人员需严格按照服务要求执行合同。

8.2 乙方为甲方提供电话技术支持服务要求为 7×24 小时。

8.3 严格遵守国家相关的法律法规、政策文件以及行业标准，确保测评活动

的合法性和规范性。

九、违约责任

9.1 因乙方的原因，造成甲方无法正常使用相关系统软件的或乙方服务达不到甲方考核要求的，甲方有权解除本合同。届时，乙方除须退还甲方已付全部合同价款外，还须按照本合同约定的合同总价款金额30%的标准向甲方支付违约金。甲方实际产生的损失超过前述金额的，乙方须另行赔偿。

9.2 如因乙方设备或软件致使甲方受到第三方追究侵犯其专利权、商标权、著作权或其他知识产权、患者隐私泄露等法律责任的，乙方应赔偿由此造成的全部甲方损失（含律师费、诉讼费等），并承担相应法律责任；如因此影响甲方正常使用设备的，按本合同9.1款约定处理。

9.3 因乙方违约导致甲方受到上级部门处罚或其它给甲方造成的损失，乙方应全额承担造成的经济损失并支付损失金额的30%作为违约金。

9.4 未经甲方同意，乙方不得擅自将本合同服务转包第三方承担。如擅自转包，甲方有权解除本合同，届时，乙方除须退还甲方已付全部合同价款外，还须按照本合同约定的合同总价款金额30%的标准向甲方支付违约金。甲方实际产生的损失超过前述金额的，乙方须另行赔偿。

十、合同文件及解释顺序

10.1 组成本合同的文件及解释顺序为：本合同及其附件、中标通知书、招标文件、投标文件。

10.2 合同履行过程中，甲方、乙方有关本项目的洽商、变更等书面协议或文件视为本合同的组成部分。

十一、合同生效及其他

11.1 合同期限届满后，合同效力自行终止，甲方相关部门无权要求乙方继续按照原合同约定履行义务，合同期限届满前30日乙方应履行书面提示义务。

11.2 合同期限届满至甲方后继采购流程完成前，确需保证原服务暂时延续的，经双方协商一致在移交空档期须另行签订补充协议。否则，在移交空档期即便乙方已按原合同约定履行义务，甲方相关部门也已认可并受领，上述行为视为乙方对甲方的无偿赠与行为，甲方有权拒绝付款，由此造成的法律后果均由乙方自行承担。

11.3 本合同未尽事宜由甲乙双方另行协商并签订书面补充协议。

11.4 发生争议双方协调解决不成的，向甲方所在地人民法院起诉。

11.5 本合同经双方代表签字并盖章后生效。

11.6 本合同一式肆份，甲方执贰份，乙方执贰份，均具有同等法律效力，合同附件及形成本项目的招标文件、投标文件、《成交通知书》均为本合同不可分割的组成部分，与本合同具有同等的法律效力。

附件一、《服务范围及要求》

附件二、《分项报价表》

附件三、《技术参数清单》

附件四、《服务承诺书》

附件五、《产品质量承诺书》

附件六、《信息系统数据安全保密承诺书》

附件七、《郑州市能源收费标准》

甲方：郑州市中心医院

地址：郑州市中原区桐柏北路 16 号

代表人：

乙方：联通（河南）产业互联网有限公司

地址：郑州市中原区华山路 105 号芝麻街 E 区 8 栋

代表人：

签约日期：2026.3.31

附件一、《服务范围及要求》

1.服务范围

本次服务范围包括网络安全等级保护测评、商用密码应用安全性评估、日常网络安全服务以及重要时期网络安全保障值守服务。围绕医院信息系统资产（包括主机、网络、应用及数据等）的建设和运行维护场景，全面落实国家网络安全等级保护和商用密码管理相关制度要求，提升医院整体网络安全防护与保障能力。

具体服务内容包括：对不少于 6 个重要信息系统开展三级网络安全等级保护测评和商用密码应用安全性评估服务；提供日常网络安全服务，配备不少于 1 名专职安全服务工程师（同时具有国家信息安全测评中心颁发的 CISP 系列认证证书及国家信息安全审查与认证中心颁发的 CISAW 系列证书），开展风险评估、渗透测试、安全咨询、应急响应及安全培训等工作；提供重要时期网络安全保障值守服务，在重要保障期间配备不少于 3 名具备攻防演习经验的重保安全工程师（具有国家信息安全测评中心颁发的 CISP 系列认证证书或国家信息安全审查与认证中心颁发的 CISAW 系列证书），实施 7×24 小时现场或远程安全监测与值守，确保医院信息系统安全稳定运行。

2.网络安全等级保护测评服务

2.1 服务内容具体要求

按照《GB/T 28448-2019 信息安全技术网络安全等级保护测评要求》、《GB/T 28449-2018 信息安全技术网络安全等级保护测评过程指南》等标准进行网络安全等级测评。具体项目测评内容如下：

安全技术测评：包括安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全管理中心等五个方面的安全测评。

安全管理测评：安全管理机构、安全管理制度、安全管理人员、安全建设管理和安全运维管理等五个方面的安全控制测评。

在安全等级测评过程中，每个工作阶段、流程、内容、及成果交付严格遵循《GB/T 28448-2019 信息安全技术网络安全等级保护测评要求》和《GB/T 28449-2018 信息安全技术网络安全等级保护测评过程指南》文件，根据本项目信息系统已完成的定级备案安全等级，开展相应级别的安全等级测评工作，根据测评结果出具相应的单项和整体测评报告，测评报告需得到项目单位的确认，并

报送网安部门。测评报告编制的内容及格式严格遵照《网络安全等级保护测评报告模版（2021 年版）》进行。

服务期间共需要完成不少于 6 个等保三级系统的等保测评工作，包括但不限于以下内容：

服务期间按公安部门要求在规定时间内协助我院准备备案材料，包括系统备案申请表、绘制拓扑图等，协助进行安全加固、完善安全管理体系建设、梳理组织架构。

服务期间按医院要求在规定时间内按照《信息系统安全等级保护测评要求》政策文件的技术要求，开展等级测评服务，遵照《信息系统安全等级测评报告模版》编制测评报告；

服务期间按医院要求在规定时间内按照《信息安全等级保护安全建设整改工作指导意见》，严格遵循《信息安全等级保护安全建设整改工作指南》各项要求，协助我院完成整改。

服务期间按医院要求在规定时间内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。

2.2 工作过程文件及项目交付成果（包括但不限于）

提交等级测评报告，完成不少于 6 个三级信息系统的等保备案。

项目阶段	交付成果
测评准备活动	项目计划书 被测系统基本情况分析报告
测评准备活动	信息系统安全测评方案
测评准备活动	测评结果记录 测评中发现的问题汇总
测评准备活动	单项测评结果汇总分析 整体测评结果汇总分析 风险分析和评估等级测评结论 信息系统安全等级测评报告

提交网络安全管理体系建议和规划，协助完善我院安全管理制度体系。

3. 商用密码应用安全性评估服务

3.1 服务内容具体要求

按照国家密码法规、密码应用相关技术标准，采用科学的测评方法、流程和工作规范开展商用密码应用安全性评估工作。供应商应具备商用密码应用安全性技术测评实施、管理测评实施、系统整体评估能力。供应商为本项目配备能够依

据测评结果做出专业判断以及出具测评报告的能力的测评人员，测评人员必须为通过国家密码管理部门（或其授权的机构）组织的考核（即商用密码应用安全性评估人员测评能力考核证书），遵守国家有关法律法规，按照相关标准，为用户提供安全、客观、公正的评估服务，保证评估的质量和效果。

服务期间共需要完成不少于 6 个三级商用密码应用安全评估工作，包括但不限于以下内容：

提供测评方案，有计划、按步骤地开展测评工作，且测评方案应专业性强，对系统现状及需求理解应准确，方案应科学合理，内容应完整、可靠性强，实施方法和技术措施应可操作性和有效性强，在签订密评合同后供应商应立即成立密评工作小组，并严格按照合同履行密评责任。

为保障密评过程中可能涉及的重要数据和敏感信息的安全，供应商应配有相关能力支撑的保密办公区，并具备安全保密管理制度与数据安全能力，采取的安全管理措施应得当，且能够很好保障本项目测评数据的安全，明确对采购人的系统、信息、数据有安全保密的义务，进场测评前必须签订保密协议。

现场测评工作中必须在不影响医院信息系统正常运行的前提下进行。

服务期间，应遵守相应的密评工作制度，包括会议制度、密评文件制度、密评记录制度、工作报告制度等，保证密评工作协调有序的进行。

服务期间，根据被测系统的具体情况，按合同约定，配备满足密评工作需要的人员、设备和工具。为保障密评实施与合同约定服务周期内的服务响应，供应商应具备一定的测评工具开发能力以及在测评服务地进行系统环境模拟实验能力。

商用密码应用安全性评估工作后，应协助我院在 30 日内将评估结果报国家密码管理部门备案。

项目验收时应提交密码安全测评工作的档案。

3.2 工作过程文件及项目交付成果（包括但不限于）

提交符合国家密码管理部门要求的商用密码应用安全性评估报告，完成不少于 6 个三级信息系统的评估结果向国家密码管理部门备案工作。

项目阶段	交付成果

实施前阶段	商用密码应用安全性评估实施方案密评工作组织及人员资质材料保密协议及安全管理文件
实施中阶段	现场测评过程文档及记录材料，包括不限于：测评实施记录、密评会议纪要、测评工作日志、测评证据材料清单和阶段性工作报告
实施后阶段	商用密码应用安全性评估报告整改建议及技术咨询成果评估结果备案支撑材料
验收阶段	商用密码应用安全性评估项目档案，包括不限于：评估实施方案、人员资质及组织材料、保密协议及安全管理文件、测评过程记录、商用密码应用安全性评估报告和备案相关材料

4.日常及重要时期安全服务

4.1 服务内容和具体要求

日常服务期间，供应商应提供不少于 1 名专职安全服务人员，且该人员须具备 CISP-PTE 认证资质；在国家级或行业级攻防演练及国家重大活动保障期间，供应商应按要求提供不少于 3 名具备攻防演练实战经验的重保安全工程师（具有国家信息安全测评中心颁发的 CISP 系列认证证书或国家信息安全审查与认证中心颁发的 CISAW 系列证书）），按照郑州市中心医院统一安排开展值班值守和安全保障工作。

主要工作：

提供服务工具：提供日志审计与分析类系统，至少能满足郑州市中心医院 500 个设备节点（如网络设备、服务器设备、应用系统及子系统等）的网络安全数据分析要求。

互联网暴露面搜集服务：对郑州市中心医院暴露在互联网上的 IT 资产进行信息搜集，判别暴露风险，结合实际业务需求，给出安全建议。

渗透测试：根据郑州市中心医院授权和需求，对全局范围内的信息系统中的主机操作系统、数据库系统、应用系统等在一年内进行不低于 4 次漏洞扫描及 2 次模拟攻击测试，要保证整个渗透测试过程都在可以控制和调整的范围之内，尽可能的获取目标信息系统的管理权限以及敏感信息，以查找和分析安全漏洞和隐患，发现应用存在的 web 安全漏洞、弱口令、中间件漏洞、信息泄露等安全漏洞，人工验证消除误报，生成相关报告并提供安全加固建议。每次渗透测试后出具正式的分析报告、解决方案、整改建议，并进行整改后的渗透性复测。

新系统上线前检测：针对新建业务系统，在新系统入网前进行检测评估，评

估方法包括漏洞扫描、安全基线检查、渗透测试等，从主机层、系统层、数 据库层、中间件层以及应用层全面评估新系统的安全状况，查找不符合安全要求的配置项以及安全风险点，并提出相应的修复方案。

应急响应：当郑州市中心医院发生安全事件时，及时提供相应的应急措施，协助郑州市中心医院限制潜在的损失和破坏；检查所受影响的系统，判定原因，并提供安全事件解决方案、排除系统安全风险、追溯安全事件来源。及时判断安全事件级别，进行紧急分析处理、灾难恢复和入侵追踪和取证，并出具应急响应报告（含加固建议）。建立长期稳定的本地专业安全服务团队，在发生重大安全事件时，在半小时内提供现场应急响应；在发生一般安全事件时，一小时内提供现场应急响应，并提交应急响应报告。

协助郑州市中心医院安全运维开展工作，包括梳理网络拓扑和现有防护措施，分析重要系统的可能攻击路径和存在的防护短板，协助加强纵深防御能力；对风险排查发现的安全隐患提供建议，输出方案，协助优化防护策略，最大程度防范安全事件的发生；在网络与信息安全专项保障和检查工作时，排查网络边界、数据、应用安全，确保重要网络和应用系统运行正常等；对监控上报的报警日志和可疑日志进行分析确认，对各安全系统发现的事件、攻击样本进行分析研判，分析研判发现的安全事件进行主动应急响应和快速处置，确保快速抑制安全事件，防止攻击方的进一步横向渗透行为。对入侵的网络安全攻击成功事件进行深度分析，并对攻击方法、攻击方式、攻击路径进行深度分析，并且撰写应急溯源报告。

重保期间提供动化攻击溯源反制类系统，对郑州市中心医院信息系统的互联网暴露面探查和检测，对可能存在数据泄露风险的互联网资产进行检测和评估，并协助对互联网侧的安全风险进行收敛和加固。

梳理重保过程、攻防演练中攻击情况和防护手段，分析防护能力、安全制度、防护流程及方案中的缺陷，商讨可落地的整改建议，并协助编写总结报告。

其它为达到安全防护要求和验收标准应当开展的工作。

4.2 工作过程文件及项目交付成果（包括但不限于）

项目阶段	交付成果
安全服务阶段	系统上线安全分析报告 互联网暴露资产清单及分析报告漏洞扫描情况、处置建议及复扫情况(每年至少四次)渗透测试报告、加固建议及复测情况(每年至少两次)整体安全工作优化方案(每年至少一次)突发情况处置报告、应急溯源报告

	等 重保或攻防演练工作方案重保攻防演练总结报告

5. 其他配套服务

以落实网络安全等级保护和商用密码安全评估制度设计初衷为目标，切实提升郑州市中心医院整体安全防护水平和安全运营能力。围绕等级保护制度中对安全运营体系建设的相关要求，在合同期内，中标单位应提供配套的网络安全类软件工具，具备高级威胁检测、日志集中审计、自动化攻击溯源与反制、资产测绘与管理、信息系统应用接口监测等功能，为医院信息系统安全稳定运行提供持续支撑。

中标单位应承诺在合同期内，根据招标人实际网络安全需求，对所提供的安全服务工具在功能配置及资源使用方面进行相应调整，包括但不限于计算能力、存储资源及授权点位等。所提供工具为纯软件形态的，在满足上述使用要求的前提下，其运行所需的硬件平台及基础资源由招标人负责配套提供。

其中自动化攻击溯源反制类系统主要功能如下表所示：

技术指标项	主要指标要求
基础要求	为保证数据安全，要求软件采用本地化方式进行部署。
风险遥测	支持对互联网暴露面风险提供可视化展示，对互联网暴露端口、暴漏服务、失活资产、敏感信息暴露、失效证书、漏洞信息、弱口令情况进行检测。
任务中心	支持基于 IP 或域名，自主创建检测任务，支持一条任务提供目标资产的资产监控、暴露面梳理、攻击面测绘任务的下发。（提供功能截图）（截图清晰可辩，能明显看出具体功能并作出标识）
资产监控	支持对互联网环境下的 IP、站点、域名等资产进行分组管理；支持统计并展示每日资产总量、存活和失活资产数、主域名资产数量、子域名资产数量、IP 资产数量、站点资产数量；提供资产指纹配置、操作系统、开放端口的 TOP 10 统计；针对 IP 类资产，提供 IP 存活状态、操作系统、重要程度、责任人等属性的检测和维护；针对站点类资产，提供站点 URL、站点标题、站点证书、站点状态、状态码、产品组件、重要程度、责任人等属性的检测和维护；针对域名类资产，提供子域名、解析类型、域名状态、关联 IP、重要程度、责任人等数据的检测和维护。
暴露面管理	提供暴露面总数、敏感信息数量、服务数量、端口数量、API 接口数量的日活可视化统计；针对互联网暴露面的开放端口、服务、协议进行统计分析；支持对单一资产提供暴露面画像，提供暴漏资产的 IP、域名、端口、服务、弱口令情况、指纹、API 接口情况、敏感信息暴露情况（包含敏感信息类型、敏感信息内容、敏感信息来源、请求方式、请求 body 等）等内容的收集和展示。（提供功能截图）（截图清晰可辩，能明显看出具体功能并作出标识）
攻击面管理	提供攻击面总数、已修复总数、超危、高危、中危、低危等漏洞数的日活可视

	化统计；提供资产视角的漏洞统计与分析；提供超危、高危、中危、低危等不同等级的各漏洞影响资产范围的统计；针对资产的高等级风险漏洞提供修复状态跟踪监控。
功能模块化管理	支持风险遥测、资产监控、暴露面管理、攻击面管理、升级管理、系统配置、用户管理和日志审计等功能模块的独立授权和管理，能够灵活按照自身需求开放和使用相关功能组件。
系统配置	支持通过 B/S 方式对产品进行管理维护，支持通过 web 方式对系统的网口配置、路由策略、DNS 配置等进行维护；支持通过 SMTP 协议提供邮件外发告警功能。

附件二、《分项报价表》

序号	货物名称	品牌型号	制造商	计量单位	数量	单价	合计	税率
1	网络安全等级保护测评服务、商用密码应用安全性评估服务、日常及重要时期安全服务、其他配套服务	联通定制	联通数字科技有限公司	套	1	1096800	1096800	6%
一	密码、电子签名设备及项目安全服务							
（一）	密码设备							
1	VPN 网关	HX-VPN V4.0	北京天地和兴科技股份有限公司	台	2	73225	146450	13%
2	服务器密码机	HX-SCM V4.0	北京天地和兴科技股份有限公司	台	1	66000	66000	13%
3	云服务器密码机	SW-CHSM V1.0	武汉思为同飞网络技术股份有限公司	台	1	153800	153800	13%
4	签名验签服务器	HX-SVS/V4.0	北京天地和兴科技股份有限公司	台	1	67650	67650	13%
5	SSL 证书	国密 OV 单域名 SSL 证书	华测电子认证有限责任公司	套	15	1000	15000	6%
6	国密浏览器	SuloongBrowser V4.0	天津赢达信科技有限公司	张	10	100	1000	13%
7	智能密码钥匙	SJK1948-G	天津赢达信科技有限公司	套	20	55	1100	13%
8	系统对接	联通定制	联通（河南）产业互联网有限公司	套	15	20000	300000	6%
（二）	电子签名							

1	协同签名服务器	BJCA COSS-A3001	北京数字认证股份有限公司	台	1	99000	99000	13%
2	协同签名 APP/协同签名 SDK/微信小程序插件	BJCA COSS-SDK-WX	北京数字认证股份有限公司	套	1	16500	16500	13%
3	时间戳服务器	BJCA TSS-HG8001	北京数字认证股份有限公司	台	1	82500	82500	13%
4	个人数字证书	BJCA CERT-U	北京数字认证股份有限公司	张/年	1500	180	270000	6%
5	设备数字证书（医务）	BJCA CERT-D-Y	北京数字认证股份有限公司	张/年	2	2750	5500	6%
6	手写信息数字签名服务器	BJCA AnySign3050W	北京数字认证股份有限公司	台	1	144600	144600	13%
7	设备数字证书（患者）	BJCA CERT-D-Y	北京数字认证股份有限公司	张/年	1	2750	2750	6%
合计金额		大写：贰佰肆拾陆万捌仟陆佰伍拾元整 小写：（2468650.00 元）						

附件三、《技术参数清单》

密码、电子签名设备及项目安全服务			
（一）	密码设备		
序号	参数	单位	数量
1、VPN网关	1.提供的VPN综合安全网关产品，采用国产海光平台，2U机箱，标配6个千兆电口，240 GSSD+2T企业级存储，配置液晶屏，带机箱锁，销售锁，冗余电源。	台	2
	2.提供的VPN综合安全网关产品并发连接数100W。		
	3.提供的VPN综合安全网关产品每秒新建连接数4W。		
	4.提供的VPN综合安全网关产品，SSL最大并发授权数2500。		
	5.提供的VPN综合安全网关产品，SSLVPN加密吞吐400Mbps。		
	6.支持国密SM2、SM3、SM4系列算法；国密算法使用硬件密码卡实现。		
	7.VPN综合安全网关产品，支持单向认证、双向身份认证，可开关选择单、双向认证模式。		
	8.支持单向认证、双向身份认证，可开关选择单、双向认证模式。		
	9.支持设置证书过滤规则，可通过对用户证书C、ST、O、CN、L、OU、Email等字段进行过滤，实现对接入用户的登入控制。		
	10.SSL并发用户数、IPSec隧道数、证书数量、CPU使用率、内存使用率、存储使用率，实时网络吞吐量。		
	11.支持国密与国际SSL双协议自适应、多站点独立证书配置，并提供参数透传URL改写及跨域等灵活的流量调度能力。（已经提供第三方权威检测机构的检测报告(封面具有CNAS标识)截图证明）		
	12.支持SM1、SM2、SM3、SM4等多种国产密码算法，适用于纯WEB应用，通过web反向代理技术。（已经提供第三方权威检测机构的检测报告(封面具有CNAS标识)截图证明）		
	13.支持基于http的WEB应用代理，支持在同一应用中添加多条代理地址，支持被代理址为https协议，支持重写重定向。（已经提供第三方权威检测机构的检测报告(封面具有CNAS标识)截图证明）		
	14.支持抗量子密钥封装机制，提供针对量子计算机攻击的防护能力。（已经提供第三方权威检测机构的检测报告(封面具有CNAS标识)截图证明）		
	▲15.提供的产品具备商用密码检测认证中心颁发的《商用密码产品认证证书》，认证级别为安全二级。（自2025年5月1日起,国家密码管理局商用密码检测中心不再开展商用密码检测认证业务，检测认证工作交由商用密码检		

	测认证中心承接。）		
2、服务器密码机	1. 提供的服务器密码机产品，采用国产海光平台，2U 机箱，标配 6 个千兆电口，240 GSSD+2T 企业级存储，配置液晶屏，带机箱锁，销售锁，冗余电源。	台	1
	2. SM2 签名性能 55000 次/秒。		
	3. SM2 验签性能 28000 次/秒。		
	4. SM3 摘要计算 1000Mbps。		
	5. SM4 加密解密 1000Mbps。		
	6. 采用经国密局批准使用的物理噪声源产生器生成真随机数，支持国密 SM2、SM3、SM4 算法。		
	7. 支持 PKCS#11 接口、JCE 接口、《密码设备应用接口规范》等国家标准接口。		
	8. 支持通过 OAuth2.0 身份认证授权标准来实现接入应用的身份校验，确认调用者身份信息，在后续的接口调用中保证身份的合法性。		
	9. 支持断链修复功能，提供在网络异常情况下加密服务中断的自动恢复。		
	10. 支持设备安全态势分析，包括密码流量分析，节点受攻击情况，异常访问情况等。		
	11. 支持“3+N”用户管理体系，满足管理员、审计员、安全员的三种用户身份设定，多个操作员配合管理的用户体系。（已经提供第三方权威检测机构的检测报告(封面具有 CNAS 标识)截图证明）		
	12. 提供针对大文件的加密接口和哈希接口，至少支持 5G 以上大文件加解密和哈希运算。		
	13. 支持对系统所有操作员的管理菜单功能权限配置。审核用户的激活和锁定状态，激活状态下该用户的权限正常使用。		
	▲14. 提供的产品具备商用密码检测认证中心颁发的《商用密码产品认证证书》，认证级别为安全二级。（自 2025 年 5 月 1 日起，国家密码管理局商用密码检测中心不再开展商用密码检测认证业务，检测认证工作交由商用密码检测认证中心承接。）		
3、云服务器密码机	一、硬件规格 提供的产品为 2U 标准机架式设备，标配 4 个千兆网络接口，采用基于国产化硬件平台的多核架构，国产化操作系统。硬件液晶屏显示。	台	1
	二、性能参数 SM1 加解密 000Mbps； SM2 密钥对生成 2w 对/秒；		

	SM2(256)签名 12W 次/秒； SM2(256)验证 2W 次/秒； SM2(256)加密 2W 次/秒； SM2(256)解密 2W 次/秒； SM3 加解密 3000Mbps； SM4 加解密 3000Mbps；		
	三、功能参数 1.可运行 16 个 VSM 虚拟密码机，每个 VSM 可对应用独立提供密码服务，并且各个 VSM 之间密钥完全隔离。		
	2.提供的产品采用经国密局批准使用的物理噪声源产生器生成真随机数；支持国密 SM2、SM3、SM4 算法。		
	3.提供的产品支持 PKCS#11 接口、JCE 接口等标准接口；支持用户定制接口的开发；支持《密码设备应用接口规范》国家标准接口。		
	4.支持断链修复功能，提供在网络异常情况下加密服务中断的自动恢复。		
	5.支持多机互备，支持应用程序配置多个虚拟密码机，实现负载均衡，多个应用服务共享虚拟密码机。		
	6.支持集群技术，云服务器密码机自身可提供高性能的密码服务，在此基础上，多台 VSM 还可以组成集群，通过集群为业务系统提供性能更高、可横向伸缩的密码服务。		
	7.支持集中管理，可对接密码云服务平台，通过可视化交互实时监控、修改配置。		
	8.支持配置证书管理模块，可为虚拟密码机和其他密码模块签发设备证书，可为虚拟机租户管理员用户签发管理员证书并通过 WEBUI 写入到 UKEY。		
	9.支持配置密码应用仿真模拟平台，可作为密码运维人员、研发人员、管理人员内部理论和实践培训平台，提供配套培训资料。		
4、签名验签服务器	1.提供的产品采用国产海光平台，2U 机箱，标配 6 个千兆电口，240 GSSD+2T 企业级存储，液晶屏，带机箱锁，销毁锁，冗余电源。	台	1
	2.SM2 P1 签名 30000 次 / 秒		
	3.SM2 P1 验签 20000 次 / 秒		
	4.SM2 P7 签名 10000 次 / 秒		
	5.SM2 P7 验签 7000 次 / 秒		
	6.提供的产品采用经国密局批准使用的物理噪声源产生器生成真随机数，支持国密 SM2、SM3、SM4 算法。		
	7.支持 PKCS#11 接口、JCE 接口、《密码设备应用接口规范》等国家标准接口。		
	8.支持 PKCS#1、PKCS#7(Attach)、PKCS#7(Detach)密码算法。		

	9.证书格式支持标准X509V3证书格式包括支持全中文证书，支持签名证书和加密证书的双证书认证体系。		
	10.支持对连接应用的访问管理，提供白名单和授权码访问控制，保障接入应用合法性。		
	11.支持通过OAuth2.0身份认证授权标准来实现接入应用的身份校验，确认调用者身份信息，在后续的接口调用中保证身份的合法性。		
	★12.提供的产品具备商用密码检测认证中心颁发的《商用密码产品认证证书》，认证级别为安全二级。（自2025年5月1日起,国家密码管理局商用密码检测中心不再开展商用密码检测认证业务，检测认证工作交由商用密码检测认证中心承接。）		
5、SSL证书	我公司提供的SSL证书，经国家密码管理局批准设立的合法电子认证服务机构(CA)签发，机构具备有效的《电子认证服务许可证》《电子认证服务使用密码许可证》证书，SSL证书能够支持身份认证，能够标识网络通讯中个人、企业、设备等的真实身份，防止攻击者假冒合法用户获得资源的访问权限，保证系统和数据的安全，以及授权访问者的合法利益。	套	15
6、国密浏览器	1.支持国密算法 SM2、SM3、SM4。在 Chrome 内核、IE 内核下均支持国密 SSL 协议。	张	10
	2.提供的产品可按应用设置选用 Chrome 内核、IE 内核，并可按应用设置 IE 内核版本，实现对现有业务系统的兼容性适配，支持 IE/Chrome 内核的自动切换与 Cookie 共享。		
	3.支持 HTML 和 CSS 解析，支持 JavaScrip 引擎，可以正确的渲染显示页面，支持基本的浏览器操作功能。		
	4.提供的产品符合 GB/T 38636-2020《信息安全技术传输层密码协议（TLCP）》。		
	5.提供的产品支持 Windows XP P3/Windows 7/Windows8/Windows10/Windows11 系列操作系统，支持 32 位、64 位。		
7、智能密码钥匙	1.提供的产品内嵌 32 位高性能、高容量智能卡芯片；自主知识产权 COS、用户存储空间不低于 128KB。	套	20
	2.提供的产品支持 2 个以上国密应用，同时支持 8 个以上证书。		
	3.提供的产品验证及运算过程在硬件内部完成，私钥永不出 Key，具有多种对抗攻击的安全检测和保护手段。		
	4.提供的产品符合 USB2.0 规范，兼容 USB1.1，兼容 3.0 规范接口。		
8、系统对接	1、对现各业务系统进行必要的改造，以支持密码设备的对接。	套	15
	2、完成密码设备与业务系统的联调测试，确保系统稳定运行		

（二）	电子签名		
1、协同签名服务器	1.采用密钥分割技术、协作签名机制，支持 SM2/SM3/SM4 等国密算法	台	1
	2.客户端与服务端分别存储密钥因子，完整密钥永不出现，提升安全性		
	3.支持 Android 、iOS 、Windows、Linux 等操作系统		
	4. 支持 CentOS、欧拉、中标麒麟、银河麒麟、UOS 操作系统，兼容主流数据库		
	5. 支持 1000 并发用户，平均签名响应时间小于 100ms，SM2 密钥生成 3000 次/秒，SM2 协同签名 7000 次/秒，SM2 验签 8000 次/秒，SM2 加密/解密 8000/7000 次/秒		
	6. 支持 AC 100-240V 电源，配备 2 个网络接口。		
	7. 具备终端设备访问控制功能，支持对移动端许可进行分配、注销、查询，通过白名单实现对应用服务器的访问授权认证。		
	8. 支持对接 CA 系统进行证书申请、颁发、验证、注销，实现 SM2 国密证书在移动端的应用		
	9.提供全流程签名记录和可追溯证据链的日志审计功能		
	10. 支持本地化部署、数据库独立部署与同步等多种部署模式		
	11.提供统一管理用户密钥与证书、支持批量导入导 出证书、监控系统运行状态与白名单配置的管理平台功能		
	12. 符合国家商用密码相关法规，遵循 GM/T 系列密 码算法标准（如 GM/T 0003-2012 SM2、GM/T 0004-2012 SM3 等），为了整机设备的稳定性与兼容性，密码卡与整机为同一厂家、同一品牌。管理员使用的管理介 质（智能密码钥匙）与设备整机为同一厂家、同一品牌。		
	★13. 已获得商用密码产品认证证书（服务端+各客户端模块）、网络安全专用产品安全检测证书资质认证。		
2、协同签名 APP/协同签名 SDK/微信小程序插件	1. 实现与微信电子签名小程序的外部联接能力。	套	1
	2. 支持医疗工作者终端的绑定、移动端的实名认证、签字收集，以及各类业务数据和文件的电子签名。		
	3. 实时签发符合《卫生系统电子认证服务规范（试行）》和卫生系统电子认证服务体系建设系列技术规范要求的第三方 CA 数字证书。		
	4. 提供用户管理功能，支持批量创建、编辑和删除用户。		
	5. 提供批量导入功能，方便管理大量用户信息。		
	6. 支持标准的 RSA/SM2 等算法，以及 Pkcs7 等格式的数字签名和验证功能。		

	7. 提供日志管理功能，用户可以查询和管理登录日志、签名日志、数据维护日志等。		
	8. 通过记录和监控日志，有助于追踪操作和保障系 统的安全性和可靠性。		
	9. 支持证书到期提醒。系统自动提醒有证书即将到期，可以查看即将到期的证书列表。		
	10. 可通过配置管进行自定义提醒周期。		
	11. 提供内网部署的移动电子签名系统。		
	12. 支持数据交换接口。		
	13. 能够接收用户实名认证请求、CA 数字证书签发和续期请求，以及文件移动电子签名请求等。		
	14. 提供外部服务数据交换接口，与微信开放平台、 CA 认证机构、国家授时中心等外部服务进行数据交互。		
	15. 支持获取用户实名认证结果、CA 数字证书签发和续期结果，以及文件移动电子签名凭证等结果。		
	16. 仅向外网提供用户身份信息和电子签名凭证信息，不涉及文件原文信息的传递。		
	17. 支持多 CA 机构数字证书签发链路的打通。		
	18. 支持集群部署模式。		
	19. 提供用户授权功能，用户可以通过小程序将自己的证书和签字授权给其他人使用。		
	20. 授权时间限制可编辑，默认授权有效期为 2 小时，		
	21. 过期后自动解除授权关系。		
	22. 提供独立电子签名应用，可直接在微信中安装和 使用。		
	23. 与院内部署的移动电子签名系统对接，能够获取和验证用户信息。		
	24. 能够与院内各信息系统对接，实现扫一扫登录认 证。		
	25. 记录带有电子签名的认证日志，确保安全性和追溯性。		
	26. 支持与院内各信息系统对接，实现扫一扫电子签名。		
	27. 支持通过数字证书对电子处方、电子病历、检验报告等文档进行电子签名。		
	28. 提供查看本人的登录认证和电子签名记录的功能。		
	29. 用户可以自定义密码策略，以满足个人安全需求。		
	30. 支持安全会话授权技术，在一定时间内免扫码自动进行电子签名。		
	31. 用户可以手动取消授权，提高用户自主控制权。		
	32. 支持微信小程序中的批量签名功能。		
	33. 可以在小程序中查看待签文件，并进行批量签名操作。		
3、时间	1. 提供字符和文件的时间戳签署和验证功能，支持对字	台	1

戳服务器	符和文件进行 SHA256、SM3 等方式的数字摘要后 再进行时间戳签署。		
	2. 提供时间戳验证、查看功能，可对签署时间戳的证书进行是否由可信颁发机构签发、是否超期、是否被吊销等有效性验证。		
	3. 提供用户业务日志、管理日志的记录。		
	4. 提供 CRL 的证书有效性验证。		
	5. 提供时间戳服务器证书管理：实现对业务系统服 务器证书的配置、更新和管理。		
	6. 动态黑名单管理：可自动更新 CRL 黑名单、动态更新，不需要重新启动服务。		
	7. 提供备份恢复功能，可通过界面备份当前所有配 置。		
	8. 提供日志记录，可将日志以 sy slog 的方式发送到指定服务器。		
	9. 支持双机、负载均衡。		
	10. 提供 c#、c++、Java、html 等开发语言和平台的接口，支持 windows、Linux 等操作系统。		
	11. 支持通过 NTP 协议调整本机时间，支持将时间源的精度、准度配置，用户作为根据能够接受的时间误差的参考。		
	12. 支持时间源管理， 以及支持对时间戳、NTP 服务的在线手工启停操作。		
	13. 支持性能扩展，提供增加硬件加密引擎或并行负载扩展方式。		
	14. 设备高度 2U； 2 个千兆网口；1 个工控电源，内存 8G DDR4 ECC 2400，硬盘 1T SATA 企业级 3.5 7200。		
	▲15. 提供《商用密码产品认证证书》。		
	▲16. 提供《网络关键设备和网络安全专用产品安全 认证证书》或《网络安全专用产品认证证书》。		
	17. 时间戳签发能力 1000 次/秒。		
4、个人数字证书	标识医护人员的网上身份。	张/年	1500
5、设备数字证书（医务）	标识服务器设备网上身份。	张/年	2
6、手写信息数字签名服务器	1. 申请和获取签名数字证书。根据签名业务及签名人鉴证信息，向电子认证服务机构证书服务平台申请 颁发用于手写签名的一次性数字证书。	台	1
	2. 通过手写数字签名终端，获取签名人手写签字笔迹，作为数字签名可视化展现效果图示。		

	3. 使用数字签名密码算法，对知情同意书进行密码运算，保护知情同意书的有效性。		
	4. 提供知情同意书的存储、归档、展现、验证举证 服务。支持知情同意书共享、同步到电子病历系统。		
	5. 支持的应用环境 Windows server2000/2003/2008/2016 等 ;Linux ;Unix 等操作系统。		
	6. 提供 C、Java 等主流开发 API。		
	7. 适用环境：千兆环境，并发用户多。		
	8. 设备高度 2U，网络接口 2x1000M，电源指标：双电源，功耗： 260W。		
	★9. 提供《商用密码产品认证证书》。		
	10. 业务处理能力 100000 笔/小时。		
7、设备数字证书（患者）	标识服务器设备网上身份。	张/年	1

附件四、《服务承诺书》

致:郑州市中心医院

联通（河南）产业互联网有限公司（以下简称本公司或供应商）是郑州市中心医院国家创伤区域医疗中心信息化建设项目密码、电子签名设备及项目安全服务供应商。

1、本公司承诺其所提供的设备均为原装正品，保证设备的完整性和可用性；提供全新的货物(含零部件、配件等)，表面无划伤、无碰撞痕迹，且权属清楚，不侵害他人的知识产权。所供产品是全新的生产日期为近期的且优质优配的。货物制造质量出现问题，乙方负责三包(包修、包换、包退)。

2、服务响应时间：提供 7*24 小时热线服务，电话服务响应时间 15 分钟内；2 小时内到达维修现场并到位检修，特殊情况在 24 小时内无法修复的，提供备用设备给用户使用。保修期内因设备性能故障检修 3 次仍不能正常使用的，乙方将无偿更换新设备。

3、质保期内提供现场免费部署、维护、升级服务；提供备品备件，发生的设备损坏、性能不合格以及设备故障无法维修时，免费提供包修、包换、包退服务；如遇软件产品升级、改版，更新及因医院业务对接需进行第三方接口开发等工作，均免费提供；同时须完成服务期内所有工作及善后服务；交付使用前发生的设备损坏和不合格，一律退换新品。

4、巡检服务：为保证所提供系统正常运行，乙方提供每年度 2 次以上不定期巡检服务，并保证所提供服务的系统的正常运行。

5、合同服务期及质保期内，免费向医院技术人员进行现场培训，内容包括软件操作、维护、基本软件的知识及简单维修，直至使医院技术操作人员能熟练掌握。

6、本公司达不到医院要求及承诺标准，在售后服务中给医院造成损失，应接受相应法律法规处罚；并承担由此造成的责任和一切经济损失。

7、服务期内对引起运行问题的软件进行检查和分析，并纠正潜在的软件缺陷或 Bug；为医院正常使用软件提供支持，如疑难解答、操作指导、系统恢复等。设备在安装调试、现场测试、试运行、终验后的质保期内及在质保期满后，因系统设计技术、设备质量等问题而影响系统正常运行或出现医院无法自行处理的问题，乙方需提供及时的技术支持。

8、本公司在质保期内提供原厂售后服务承诺。

乙方：联通（河南）产业互联网有限公司

授权代表人：

附件五、《产品质量承诺书》

致:郑州市中心医院

联通（河南）产业互联网有限公司是郑州市中心医院国家创伤区域医疗中心信息化建设项目密码、电子签名设备及项目安全服务供应商。

我单位承诺所提供产品及服务合格，符合国家、行业及地区相关标准规范，满足采购人及相关部门的质量要求。质保期：自项目竣工验收合格后，软件 1 年免费质保，硬件 3 年免费质保，且完成在服务期内所有工作及善后服务。

特此承诺！

乙方：联通（河南）产业互联网有限公司

授权代表人：

郑州市中心医院

附件六、《信息系统数据安全保密承诺书》

致:郑州市中心医院

联通（河南）产业互联网有限公司（以下简称本公司或供应商）是郑州市中心医院国家创伤区域医疗中心信息化建设项目密码、电子签名设备及项目安全服务供应商。本公司对于与郑州市中心医院信息项目合作过程中产生的业务核心数据、数据库内容、系统账号及口令、产权专利等负有保密责任，对此，本公司承诺如下：

一、保密的信息

本公司承诺予以保密的“保密信息”是指郑州市中心医院以任何情形（包括但不限于：书面，口头，或以样品、范本、计算机程序或其他形式）向供应商披露的任何信息和资料，以及本公司聘用的工作人员在工作中接触的一切属于郑州市中心医院的信息和资料，以及信息系统所收集的患者资料的所有信息数据库以及调用数据库的所有功能模块，包括但不限于：

1. 与技术有关的网络拓扑结构、网络配置协议、安全设备部署结构及详细参数、安全软件及业务平台架构方式、实际部署结构、使用技术参数、系统开发文档、配置文档、业务软件及软件源代码、系统管理手册、知识产权信息及产品专利等任何或所有的技术秘密。

2. 与运维管理有关的信息化规划、内部管理规章制度及涉密文件、各类设备及系统的运维账号、密码、密码管理策略、日志数据、用户手册等任何或所有的运维管理秘密。

3. 与业务有关的信息化项目方案、信息化项目合同、办公、财务、人事、企管等任何或所有涉及披露方业务的各类数据资料。

4. 与研究、开发、生产、产品、服务、客户、市场有关的软件、程序、发明、工艺、设计、图纸、专有技术、工程、流程、方式、硬件配置信息、客户名单、员工信息、合同、价格、成本、研究报告、预测和估计、报表、商业计划、商业秘密、商业模式、公司决议等任何或所有的商业信息、财务信息、技术资料、生产资料以及会议资料和文件。

5. 本公司以任何形式全部或部分从保密信息中获得的任何记录、总结、报告、分析或其他材料均应被视为保密信息。

6. 关于业务系统的数据库的全部信息。

7. 其他经郑州市中心医院确定应当保密的事项。

8. 虽然不属于上述所列情形，但信息自身性质表明其明显是保密的。

二、供应商的保密责任

1、供应（服务）商及供应商项目组工作人员无论主观上存在故意或者过失，都不得采取任何形式、通过任何手段违反保密义务，包括但不限于：数据库管理员权限进行数据统方统计查询、将内网服务器 ip 地址、密码、数据库账号密码泄露给第三方、将郑州市中心医院核心业务数据泄露传播给第三方、对郑州市中心医院业务数据进行不正当的操作、将郑州市中心医院业务数据带出院外等。

2、供应商应对所属相关人员进行安全保密教育，遵守本承诺书，杜绝出现人员泄密情况。

3、供应商有义务对所上线系统服务器及数据安全进行安全配置，杜绝一切安全漏洞。

4、供应商应将系统可能存在的各种安全风险如实告知郑州市中心医院。

5、供应商对上线系统要实时跟踪服务，对系统自身存在的安全技术缺陷风险、计算机技术水平发展中所带来的安全风险等，应随时查漏补漏，以保证计算机的安全运营。

6、业务系统功能需要测试的，运行环境和数据只能放郑州市中心医院院内，用于系统测试或项目推进过程中获取的数据，应当在系统测试完成或项目验收后即刻消毁，并报郑州市中心医院信息安全管理部门备案。

7、未经郑州市中心医院信息安全管理部门批准严禁从郑州市中心医院所有的服务器、存储阵列、电脑等设备中拷贝任何信息数据和资料，擅自拷贝以属于盗窃。

三、供应商的项目相关工作人员的保密责任

1、不得以任何方式向医院内外无关人员（包括家庭成员）和通信中散布、泄漏医院机密或涉及医院机密。

2、所有在工作中制作的数码、影像制片，均属于郑州市中心医院所有。禁止私自制作与复制。

3、所有在郑州市中心医院电脑、服务器及存储系统中创建、存贮和交流的信息，均属于郑州市中心医院所有。禁止利用郑州市中心医院系统电脑资源以郑州市中心医院或个人名义发表虚假信息或泄露郑州市中心医院机密。供应商需对采用电脑技术存取、处理、传递的郑州市中心医院机密资料负保密责任。

4、供应商项目工作人员离岗离职时，应将工作时使用的电脑、U 盘等其他一切存储设备中关于医院信息化工作相关或与医院信息科有利益关系的信息、文件等内容交接给医院信息科主任，并填写交换记录表，不得在离岗离职后以任何

形式带走相关信息。

5、严禁供应商利用院内医疗信息管理系统为医药营销人员提供医生临床用药情况等医疗信息。

6、不在涉密计算机上联接和使用非涉密用存储设备；不在非涉密计算机上联接和使用涉密移动存储设备。

7、不将涉密计算机和涉密移动存储设备带至与工作无关的场所。确需携带外出的，必须经郑州市中心医院主管领导批准。

8、其他可能损害郑州市中心医院信息安全行为。

9、定期接受郑州市中心医院的信息安全教育、并接受信息安全保密审计。

四、保密的期限

本公司承诺，本公司及项目工作人员承担保密责任的期限为永久。

五、违约责任

本公司及项目相关工作人员须严格遵照本承诺书履行保密义务，若有违反承诺之行为则视为违约，由本公司承担相应责任，并赔偿郑州市中心医院由此产生的损失，损失赔偿按照如下方式计算：

1、损失赔偿额为郑州市中心医院因供应商的违约行为所受到的实际经济损失。

2、如果郑州市中心医院的实际损失难以计算的，损失赔偿额为供应商因违约行为所获得的全部利益；郑州市中心医院实际产生的损失超过前述金额的，乙方须另行赔偿。

3、因供应商违约导致郑州市中心医院受到上级部门处罚或其它给郑州市中心医院造成的损失，供应商应全额承担造成的经济损失。

4、郑州市中心医院因调查供应商的违约行为而支付的合理费用包含在损失赔偿额之内。

特此承诺！

乙方：联通（河南）产业互联网有限公司

授权代表人：

附件七、《郑州市能源收费标准》

郑州市能源收费标准

单价：元

序号	能源类别	单位	收费标准	备注
1	水	立方	5.95	
2	电	度	0.7	
3	热力	平米/天	0.28	

如有最新政策，按新政策执行