众阳健康
MOUNHEALTH

合同编号：_____

云资源运维及项目维护

服务费合同

项 目 名 称：襄城县医疗健康集团区域云资源使用及信息系统运维服务项目合同

甲方（买方）：襄城县人民医院

乙方（卖方）：众阳健康科技集团有限公司

甲乙双方根据相关法律规定，本着平等互利、诚实信用的基本原则，经协商一致，就甲方向乙方关于医院信息系统售后服务费事项达成以下合同条款，以资共同遵守。

第一条 服务内容、期限、金额

1.1 服务项目所在地点：襄城县医疗健康集团。

1.2 服务内容：详见附件一、附件二

1.3 服务方式：

（1）远程支持：乙方客户服务人员通过《客户服务系统》，远程解决甲方提出的技术问题。

（2）电话支持：乙方客户服务人员通过客服电话，解决甲方提出的技术问题。

（3）现场维护：乙方派遣技术人员到甲方指定现场解决远程服务无法解决的问题。

（4）系统维护：根据甲方要求乙方在不改变原系统整体结构的前提下对原系统进行相应的调整，调整的内容须由双方协商一致后确定。

（5）接到甲方《客户服务系统》提出关于软件的服务请求后，在48小时内给予响应并提供服务。

1.4 本项目服务期限为三年，实行一年一考核一签合同。

1.5 本合同为第一年服务合同，自2026年7月28日起至2027年7月27日止。

1.6 本合同总价款为（含税）￥ 118万元整（大写：壹佰壹拾捌万元整 ），其中增值税税额为66792.45元：

第二条 双方权利和义务

2.1 甲方权利和义务

2.1.1 甲方应提供乙方工作所需环境；甲方所提供的前述环境是否合格应经双方书面确认。

2.1.2 甲方应向乙方提供并允许乙方为软件项目的维护服务工作目的而使用合同双方商议确认的信息、数据、资料。

2.1.3 甲方有权监督本项目的维护服务工作过程，并指派授权人 魏国军 对于乙方按照合同约定所完成工作内容予以确认。甲方如变更授权人，应提前15工作日书面通知乙方变更后的授权人信息。

2.1.4 如乙方履行本合同过程中需要与第三方进行配合的，甲方应负责协调乙方与第三方的工作。

2.1.5 甲方应按本合同第三条的约定向乙方支付款项。

2.1.6 甲方的其他权利和义务：\。

2.2 乙方权利和义务

2.2.1 乙方保证软件项目的维护服务工作符合合同约定的质量要求。

2.2.2 乙方保证其现场软件项目的维护服务人员拥有从事本项目维护服务工作的资格和水平。

2.2.3 乙方保证在合同履行过程中不侵犯第三方知识产权。

2.2.4 乙方人员在甲方现场工作期间,应严格遵守甲方的有关规章管理制度。

2.2.5 乙方提供服务所配置人员与甲方无任何劳务关系，甲方不承担任何义务和责任。

2.2.6 乙方在合同维护有效期内提供众阳软件系统技术服务与技术支持。

2.2.7 乙方的其他权利和义务：\。

第三条 付款及开票

3.1 合同签订后乙方开具本年度合同服务费金额发票，甲方在收到发票的30个工作日内支付年度合同服务费价款的50%，即59万元整（大写：人民币伍拾玖万元整），年度服务期限

结束后支付年度合同服务费价款的50%，，即59万元整（大写：人民币伍拾玖万元整）。

3.2 甲方应将货款电汇至以下乙方账户：

开　户　名　称：　众阳健康科技集团有限公司
开　　户　　行：　中国工商银行济南自贸区新泺大街支行
银　行　帐　号：　1602160219000270685

3.3 乙方应向甲方提供相应的、符合国家规定的增值税普通发票。甲方的开票信息：

公 司 名称(全称)：　襄城县人民医院
统一社会信用代码：　12411025417025369W
开　户　银　行：　中国建设银行股份有限公司襄城支行
银　行　账　户：　41001560810050203116
地　　址：　襄城县中心路2119号
电　　话：　0374-3592077

第四条 知识产权及保密

4.1 乙方依照本合同向甲方交付的工作成果的知识产权归乙方所有。甲方享有非独占且不可转让的内部使用权。

4.2 在本合同签订前已经存在的或履行过程中产生的其他成果，包括但不限于设计方案图纸、各种说明书、测试数据资料、计算机软件、技术诀窍以及其他技术文档，知识产权归属原创权利人所有。

4.3 甲乙任何一方应对在本合同签订或履行过程中所接触到的对方的一切保密信息，包括但不仅限于前述的知识产权信息、技术资料、技术诀窍、业务经营信息、内部管理方法、内部规章制度以及其他与企业经营相关的信息，负有保密义务。未经对方的事先书面同意，不得进行任何形式的使用或者透露给任何第三方。本合同终止后，一方将立即归还从对方处获得的一切保密信息，或者以对方认可的方式进行销毁。

4.4 保密期限不受本合同期限的限制，在本合同履行完毕后10年内，保密信息接受方仍应承担保密义务。

第五条 违约责任

5.1 甲乙双方任何一方不履行本合同义务或者履行本合同义务不符合合同约定的，均视为违约。违约方应当承担继续履行、采取补救措施或者赔偿损失等违约责任。

5.2 甲乙双方在完成双方签署的书面确认事项后，任何一方提出变更要求，导致项目进度延迟的，不视为对方违约；因此而给对方造成损失的，由提出变更一方承担相应的责任。

5.3 因甲乙双方任何一方的原因致使另一方遭受第三方追诉的，违约方应赔偿由此给另一方造成的损失。

5.4 甲方未按约定时间履行付款义务的，甲方应承担违约责任，每逾期一日，按应付未付款的0.1%向乙方支付违约金，违约金总额不得超过逾期款项的10%，由此导致项目进度延迟的，双方应重新协商项目进度安排并予以书面确认。

5.5 因甲方的原因或与甲方具有协作关系的第三方的原因导致项目进度延迟的，乙方不承担违约责任，因此而给乙方增加工作量的，甲方应按照双方协商一致的确认结果给予补偿。

5.6 因乙方原因造成不能按约定时间进行本合同履约的，乙方应承担违约责任，每逾期一日，按应付未付款的0.1%向甲方支付违约金，违约金总额不得超过逾期款项的10%。违约金的支付并不能免除乙方继续履行合同的义务。

5.7 违约方的全部赔偿责任，包括但不限于因合同、侵权、违约或者违反保证或其他引起的赔偿，累计不超过本合同总价款的20%。

第六条 责任限制

6.1 在任何情况下，乙方无须就下列情形承担责任：

（1） 第三方对甲方提出的索赔要求，但依本合同约定应由乙方承担的除外；

（2） 乙方已交付的合同系统和技术资料的丢失或损害，或已交付的合同系统因系统使用者操作不当及其他不可归责于乙方的原因，导致的数据丢失、设备损坏或其他损失；

（3） 因甲方使用非本合同约定的第三方软件或设备导致的系统无法正常运行；

（4） 因不能预见的政府行为，包括但不限于国家政策、法律、法规的限制，导致合同无法部分或全部履行或履行迟延；

（5） 甲方的任何间接经济损失；

（6） 其他______。

6.2 在任何情况下，甲方无须就下列情形承担责任：

（1）第三方对乙方提出的索赔要求，但依本合同约定应由甲方承担的除外；

（2）乙方的任何间接经济损失；

（3）因乙方原因导致数据丢失或泄密所产生的经济损失；

（4）其他 \ 。

第七条 不可抗力

7.1 本合同中不可抗力指地震、台风、火灾、水灾、战争、罢工以及其他双方不能预见、不能避免并不能克服的客观情况。

7.2 由于不可抗力致使合同无法履行的，受不可抗力影响一方应立即将不能履行本合同的事实书面通知对方，并在不可抗力发生之日起十五日内提供相关证明文件。

7.3 本合同在不可抗力影响范围及其持续期间内将中止履行，本合同执行时间可根据中止的时间相应顺延，双方无须承担违约责任。不可抗力事件消除后，双方应就合同的履行及后续问题进行协商。如果不可抗力原因造成本合同中止履行超过90个工作日，任何一方均有权解除合同。

7.4 一方迟延履行后发生不可抗力的，不能免除责任。

第八条 争议解决方式

8.1.本合同适用中华人民共和国法律。

8.2.凡因本合同引起的或与本合同有关的任何争议，合同双方可通过协商解决，协商不成，按照以下第（一）种方式解决：

(一)向甲方所在地人民法院起诉。

(二)将争议提交甲方仲裁委员会并按照申请仲裁时该会现行有效的仲裁规则进行仲裁。仲裁裁决是终局的，对双方均有约束力。

8.3. 在诉讼或仲裁期间，本合同不涉及争议的条款仍须履行。

第九条 合同的变更、转让和终止

9.1 本合同一经生效，非经甲乙双方书面同意，任何一方以任意方式对合同条款的增减及其他变更均无约束力。

9.2 非经一方书面同意，另一方无权转让本合同及该合同约定的全部或部分权利、义务。

9.3 甲乙双方全部履行合同及相关附件约定的义务后，本合同自然终止。本合同及相关附件任何条款之法律效力于尚未终止前，均及于双方当事人和各自的承继人、受让人。

9.4 任何一方如进入破产程序，另一方有权解除本合同，但必须以书面通知对方。

第十条 其他

10.1 本合同书一式肆份，甲方贰份，乙方贰份，自双方加盖公章或合同章之日起生效，原件、传真及扫描件具有同等法律效力。

10.2 除双方在合同中约定的条款外，其他未尽事宜均以合同附件或其他形式另行约定，并构成本合同不可分割之组成部分。本合同的内容及其有关的附件是甲乙双方关于此次合作所最终确定的全部内容，双方均承认其已审阅、理解本合同及相关附件的内容。

10.3 本合同各条款的标题只是为了阅读和援引方便而设立，当某个条款具体内容与标题的含义不一致时，不影响该条款具体内容之效力。乙方有责任采取措施防止云端数据泄露、丢失、非法篡改，但对非乙方原因导致的后果乙方不付相应责任，甲方所有存储在乙方云健康上的数据所有权归甲方，未经甲方授权乙方不能将甲方数据提供给第三方使用。为了确保数据安全，乙方向甲方提供云健康平台数据的本地备份及相关说明文档，甲方可在本地备份库中对医院数据进行查询、导出。乙方应积极配合甲方采购的第三方系统接入云健康系统，甲方应协调第三方系统按照云健康统一的接口标准接入到云健康系统。

10.4任何一方未行使其于此合同项下的任何权利均不得构成或被视为该方对这些权利或其它权利的放弃或丧失。

10.5 如果此合同中的任何条款或约定被认为非法或不可执行，则除这些条款和约定以外的其他条款的效力和可执行性不得因此而受到影响。

10.6合同未约定的，以招标文件为准；招标文件未约定的，以投标文件为准。招标文件和投标文件是本合同不可分割的组成部分，与本合同具有同等法律效力。双方应严格遵守招标文件和投标文件中的各项规定和承诺。

（以下无正文，为签字区）

甲方（盖章）：

签订日期：2026.7.28

乙方（盖章）：

签订日期：2026.7.28

附件一：分项报价表

序号	名称	品牌	服务期限	单价（元）	合价 （单价×数量，元）
1	云资源使用	无	1 年	585000.00	585000.00
2	信息系统售后服务及数据接口对接、性能优化提升	无	1 年	595000.00	595000.00
总报价（元）		1180000.00			

附件二：云运维服务清单

1.总体要求

应支持基于业界主流的微服务架构体系进行开发和建设，运维人员应具有丰富的云平台运维管理和具备故障排查解决经验，确保能够解决、修复所使用的软件中的问题。

2.基础服务

（1）应提供业务系统所需的整体计算能力和业务承载能力保障。

（2）云平台可靠性服务：应支持在容错、故障、攻击等场景下，通过冗余、高可用集群、应用与底层设备松耦合等特性来体现，从硬件设备冗余、链路冗余、应用容错等方面充分保证整体系统的可用性，来实现系统在故障或攻击时服务的正常使用或服务降级时的核心服务确保一定的服务能力。应能够快速恢复故障应用系统，确保业务的连续性。

（3）云平台建设服务：应支持对云平台上业务系统的整体建设，对各个业务系统模块建设资源应支持具体动态调整、网络支持动/静态BGP接入、支持x86及异构算力等保证业务平稳健康运行满足业务需求。应提供计算、存储、网络、安全、容器、数据库、中间件、大数据、人工智能、物联网等多种服务能力，满足当前及未来业务的扩展。

（4）云平台高可用性服务：云平台业务系统建设过程中所需的中间件支持，应提供稳定的消息队列服务支撑、稳定的高速缓存存储能力支撑、大数据量写入存储能力支持、大数据量日志的数据搜索引擎能力支撑等。

（5）云平台服务系统持续集成与持续发布，应支持为整个业务系统敏捷版本发布提供稳定的持续集成与发布能力，提供无故障感知的服务升级能力，提供服务升级灰度发布以及滚动升级能力。

3.安全服务

（1）应支持为云服务器、云容器、云数据库等云上资源构建隔离、私密的虚拟网络环境。VPC丰富的功能应支持灵活管理云上网络，包括创建子网、设置安全组和网络ACL、管理路由表、申请弹性公网 IP和带宽等。通过链路冗余，分布式网关集群，多AZ部署等多种技术，保障网络的安全、稳定、高可用。

（2）安全组：应支持为云上虚拟服务器设置合理的安全组管理策略，内网之间仅允许指定业务端口开放。安全组是一个逻辑上的分组，应支持为具有相同安

全保护需求并相互信任的云服务器、云容器、云数据库等实例提供访问策略。安全组创建后，应支持在安全组中定义各种访问规则，当实例加入该安全组后，即受到这些访问规则的保护。

（3）Web应用防火墙（WAF），应支持七层HTTP协议的防护策略支持，使用WEB应用防火墙或其他防护手段，对常见的SQL注入、跨站脚本攻击等进行防御。

应支持对网站业务流量进行全方位检测和防护：HTTP (S)请求进行检测，识别并阻断网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC攻击、恶意爬虫扫描、跨站请求伪造等攻击，保护Web服务安全稳定；提供精准高效的威胁检测、针对业界爆发的高危web漏洞，应提供快速分析漏洞、向引擎下发漏洞防御规则的支持，保障0day漏洞及时在waf打上虚拟补丁，用户无感知；应支持通过Web应用防火墙服务配置地理位置访问控制规则。可针对指定国家、省份的来源IP 自定义访问控制；提供简洁友好的控制界面，实时查看攻击信息和事件日志。

（4）企业主机安全，应对云上资源建设主机防护措施，对主机安全行为进行监控，对于恶意注入的木马、病毒等能够扫描并干预。应提升主机整体安全性的服务，提供资产管理、漏洞管理支持检测系统和软件漏洞、Web-CMS漏洞，识别潜在风险。入侵检测、基线检查等功能，降低主机安全风险；检测系统中的口令复杂度策略，给出修改建议，帮助用户提升口令安全性；对运行中的程序进行检测，识别出其中的后门、木马、蠕虫和病毒等恶意程序，帮助用户识别出系统存在的安全风险。

（5）云堡垒机，应支持对云上服务器的操作运维审计；提供云计算安全管控的系统和组件，包含部门、用户、资源、策略、运维、审计等功能模块，集单点登录、统一资产管理、多终端访问协议、文件传输、会话协同等功能于一体。通过统一运维登录入口，基于协议正向代理技术和远程访问隔离技术，实现对服务器、云主机、数据库、应用系统等云上资源的集中管理和运维审计；提供可视化运维行为监控，及时预警发现违规操作；实时记录管理员的资源管理、用户管理和策略管理等所有行为日志，以便监控和审计。

（6）数据库安全服务，审计数据库操作行为。应支持对数据库的内部违规和不正当操作进行定位追责，保障数据资产安全。

（7）安全态势感知，应支持统一的威胁检测和风险处置平台；应支持检测

出8大类的云上安全风险，包括DDoS攻击、暴力破解、Web攻击、后门木马、僵尸主机、异常行为、漏洞攻击、命令与控制等。利用大数据分析技术，态势感知可以对攻击事件、威胁告警和攻击源头进行分类统计和综合分析，呈现全局安全攻击态势。

（8）云审计，应支持对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等，记录审计日志、审计日志查询、审计日志转储。

（9）云监控，应支持一个针对弹性云服务器、带宽等资源的立体化监控平台。资源使用情况、业务的运行状况，并及时收到异常告警做出反应，保证业务顺畅运行。

（10）云日志，应支持日志收集、实时查询、存储等功能，通过海量日志数据的分析与处理，可以将云服务和应用程序的可用性和性能最大化，提供实时、高效、安全的日志处理能力。

4.云资源日常运维服务

（1）专门的运维团队，应支持全时段运维服务，制定科学的管理制度、服务流程、质量管控策略等，形成稳定高效的服务管控体系，做到管理规范、流程合理、职责明确、服务高效。

（2）监控服务：云平台基础资源的实时监控与告警，应包括云主机计算资源、内存资源、存储资源等维度的实时监控与分析，对日常业务运行提供业务异常监控，对日常网络带宽提供预警监控，对以上所有监控维度的实时监控与实时告警能力支撑。

（3）云平台故障处理服务：应支持根据业务运行需要，对云平台各组件、各项参数进行针对性的调优，如调整资源虚拟化比例、虚拟CPU类型与型号、服务线程数量，对业务运行过程中的故障进行分析监测，故障解决，提供7x24的检测与处理能力。

（4）云平台容量规划与调整服务。应支持对业务需求统计分析，对云平台进行容量规划，包括计算能力、存储容量、网络IP地址空间等；实施网络隔离，保障网络安全。

附件三：项目维护服务清单

1.信息规划：提供医疗信息化规划建设咨询。主要包括根据甲方信息化建设目标，目前待解决的难点痛点问题，从信息化建设角度提出相关规划方案及建议。

2.培训和支持：有针对性对相关科室进行强化培训，主要包含软件最新版本功能介绍、日常操作注意事项、常见问题处理方法等。

3.系统运维：设固定专职常驻客服人员 1 人，另在采购方办公地点设运维常驻人员不少于1人，跟踪负责解决客户的所有问题。以上专员需熟悉区域信息系统相关工作，并跟踪客户问题的沟通解决进度，定期将客户所提交客服问题汇总整理并以邮件或微信形式发送客户指定负责人，内容包括问题详述、处理办法、处理进度、完成时间或预计完成时间等。系统维护响应时间及处理时间如下：

问题类型		响应时间	处理时间
业务运行类		实时沟通及分配	实时电话和微信沟通，一般问题及时处理，复杂问题及时提出解决时间及方案。
业务终止类		1天内分配	优先远程，3小时内无法恢复立即协调相关人员根据院方要求以最快的方式到现场
日常客服问题	新增表单、报表类	2天内分配	10天内处理完毕，并反馈至信息科
	报表、表单修改类	2天内分配	5天内处理完毕，并反馈至信息科
	数据修改提取、对账类	2天内分配	7天内处理完毕，并反馈至信息科
	故障排查类（针对软件类）	1天内分配	5天内处理完毕，并反馈信息科排查结果
	转研发类	2天内分配	依照需求管理规范
	接口类	2天内反馈	根据合同中约定

4.接口服务：供应商为采购人提供现行第三方信息系统及后续第三方信息系统的长期免费对接。

5.区域信息系统模块版本架构内的性能优化提升，BUG修复等。