合同编号：_____

云资源使用及信息系统运维服务合同

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、乙双方关于医院云资源使用及信息系统运维服务费事项特立本合同，以资共同遵守。

第一条 服务内容及价格

服务项目所在地点：襄城县人民医院。

服务内容详见：附件 1、附件 2

本合同总费用为（含税）￥142.8 万元/年（大写：人民币壹佰肆拾贰万捌仟元/年）增值税税额为 80830.19 元。其中：云资源使用费（服务内容详见附件 1）￥72.8 万元/年（大写：人民币柒拾贰万捌仟元/年）；信息系统运维服务费（服务内容详见附件 2）￥70 万元/年（大写：人民币柒拾万元/年）。服务期限为 三 年，实行一年一考核一签合同。

本合同为第一年服务合同，自 2025 年 8 月 22 日起至 2026 年 8 月 21 日止。

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，包括软硬件环境、工作场所；甲方所提供的前述环境是否合格应经双方确认。

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 于大海 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 乙方应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 乙方应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 乙方应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,应严格遵守甲方的各项规章管理制度。

2.2.5 乙方在合同维护有效期内提供本项目的云资源使用及信息系统运维服务。

2.2.6 乙方的其他权利和义务：\。

第三条 付款及开票

3.1 云资源使用部分：甲方应在本合同生效并收到乙方发票的 15 个工作日内以电汇方式向乙方支付本合同云资源使用费的 95%的款项，即 69.16 万元整（大写：陆拾玖万壹仟陆佰元整），本合同服务期限结束后支付 5%的尾款，即 3.64 万元整（大写：叁万陆仟肆佰元整）。

信息系统运维服务部分：甲方应在本合同生效并收到乙方发票的 15 个工作日内以电汇方式向乙方支付本合同信息系统运维服务费 50%款项，即 35 万元整（大写：人民币叁拾伍万元整）；剩余款项 50%在一年服务期满前，经双方验收通过后以电汇方式向乙方支付 35 万元整（大写：人民币叁拾伍万元整）。

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 服务续期

1.次年度服务合同续签前，需在本次服务合同结束前 30 日内完成考核，考核通过后签约次年度服务合同。

2.甲方未按照本合同约定支付相应服务费的，乙方可书面通知甲方，甲方在收到乙方书面催款通知 15 个工作日后仍未支付相应服务费的，乙方可终止服务，由甲方自行承担由此造成的全部责任。在甲方支付服务费后，乙方将继续提供服务。

第五条知识产权及保密

5.1 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。

5.2 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，包括但不限于业务数据资料、测试数据资料、操作说明及其他技术文档，知识产权归属原创权利人所有。

5.3 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信息保密，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信息，或者以对方认可的方式进行销毁。

5.4 保密期限不受本合同期限的限制，在本合同履行完毕后30年内，保密信息接受方仍应承担保密义务。

第六条 服务终止

6.1 若甲方在服务期满后不继续使用乙方服务或服务期内解除本合同，甲方需提前一个月书面通知乙方并做好衔接安排，乙方无偿配合甲方进行全量数据的迁移，并确保迁移数据完整可用。若甲方原因导致数据迁移在服务终止前未能完成的，甲方可申请服务延长一定期限，在甲方向乙方支付服务延期的费用后，乙方提供延期服务；若乙方原因导致数据迁移在服务终止前未能完成的，甲方可申请服务延长一定期限直至数据完全迁移，在此期间产生的服务费甲方不予承担。乙方在合作终止后将不再保留甲方所有业务数据，相应数据将被彻底删除，包括缓存或者备份的副本，甲方应当自行承担其数据被删除的一切后果。

6.2 若因本合同约定的服务终止导致甲方其他服务不可用或受到影响的，乙方不承担任何责任，甲方需在本服务终止前提前做好计划安排。

第七条 合同的解除

发生下列情形之一时，甲方有权以书面通知的方式单方解除本合同，合同自乙方收到甲方的书面通知之日起终止。甲方据此解除合同不构成违约，无需向乙方支付任何违约金：

7.1 重大违约及持续违约：

乙方未能履行本合同项下的任何主要义务（包括但不限于第2.2.1、2.2.2、2.2.5条及附件约定的核心服务义务），经甲方发出书面通知后15个工作日内仍未纠正的；

乙方在合同有效期内累计 3 次发生未能达到附件中约定的服务响应或处理时间标准等违约行为，经甲方书面通知后仍未做出实质性改进的。

7.2 重大安全事故：

因乙方原因发生重大数据泄露、丢失、毁损或网络安全事件，对甲方业务运营、患者信息安全或声誉造成重大不利影响的；

乙方提供的服务存在重大安全漏洞，且在甲方通知后合理期限 3 个工作日内未能有效修复或提供可接受的应急方案的。

7.3 知识产权侵权：

乙方向甲方提供的服务、软件或工作成果侵犯第三方知识产权，导致甲方无法正常使用服务或面临诉讼、索赔风险，乙方未能在甲方指定的合理期限内解决此侵权问题或为甲方取得合法使用权的。

7.4 资信与经营状况恶化：

乙方进入破产、清算、解散程序，或其主要资产被接管、查封，或无法正常经营，导致其无法继续履行本合同项下义务的；

乙方发生重大股权变更或核心团队变动，且甲方有合理理由认为该变更将对其履行本合同的能力产生严重不利影响的。

7.5 违反合规与法律要求：

乙方的行为严重违反其在本合同项下的保密义务；

乙方未能遵守其承诺的数据安全与个人信息保护义务，导致甲方面临重大合规风险且未能在甲方要求的时间内完成整改的。

第八条 违约责任

8.1 甲乙双方任何一方不履行合同义务或者履行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，违约方应承担守约方因追讨违约方的违约责任所支出的各项费用（包括但不限于律师费、诉讼费、保全费、财产保全担保费等）。

8.2 服务期未届满，甲方违反合同约定提前终止合作的，属于甲方违约，应承担违约责任，违约金额为本年度剩余服务费用，同时甲方已支付的服务费用不予退还。甲方因违约应向乙方支付的赔偿上限不超过合同总金额的 20%。

8.3 如果因乙方违反合同约定提前终止合作的，属于乙方违约，乙方应向甲方支付违

约金，违约金数额为甲方已向乙方支付金额的 20%，同时给甲方造成经济损失的，应按损失金额承担赔偿责任。

第九条 特别说明

9.1 甲方在乙方服务规则允许的范围内对其业务数据进行删除、更改等操作，但应当谨慎操作。如甲方删除数据的，乙方按照甲方的指令不再保留相关数据，甲方数据一经删除，即不可恢复，甲方应承担数据因此被删除所引发的后果和责任；甲方理解并同意，乙方没有继续保留、导出或者返还甲方数据的义务。

9.2 乙方提供的服务可能因甲方人员非法操作，或互联网和电子通信固有的缺陷而产生限制、延迟和其它问题，亦可能因政府的管制规定而暂停或调整服务，或因黑客攻击导致网络瘫痪，或因行业技术水平所限出现无法避免的瑕疵，或其他第三方产品或服务故障导致乙方产品瑕疵或不可用等。如出现以上非乙方原因造成的任何延误、错误或其它损失时，甲方可申请双方共同协商或向甲方所在地人民法院提起诉讼，用以确定双方承担的责任比例。

9.3 乙方应采取（并将根据技术的发展不断完善）必要的技术措施来防御包括但不限于计算机病毒、网络入侵和攻击破坏等危害网络安全事项或行为，但鉴于网络安全技术的局限性、相对性以及该等行为的不可预见性，因此如网站遭遇攻击等行为而给乙方或者乙方的其他网络或服务器带来危害，乙方可决定暂停或中止服务。若给甲方造成损失的，甲方可申请双方共同协商或向甲方所在地人民法院提起诉讼，用以确定双方承担的责任比例。

9.4 甲方理解并认可，乙方依照法律法规要求对其系统、设备等采取基础的安全保护措施，确保为甲方提供符合合同约定的运行及维护服务，保证甲方正常经营。

9.5 乙方尽最大努力确保系统的可靠性、稳定性，但鉴于计算机、互联网的特殊性，下述情况不属于乙方违约：（1）乙方在进行系统及服务器配置、维护、升级时，需要短时间中断服务；（2）由于 Internet 上的通路阻塞造成甲方访问网站速度下降。

第十条 争议解决方式

10.1. 本合同适用中华人民共和国法律。

10.2. 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)将争议提交甲方所在地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。

10.3. 在诉讼或仲裁期间，本合同不涉及争议的条款仍须履行。

第十一条 其他

11.1 本合同的订立及履行过程中不得违背招标文件的实质内容，招标文件、投标文件及本合同的未尽事宜双方另行协商，达成一致后签定补充协议，补充协议和附件是本合同不可分割的整体。

11.2 本合同替代此前双方所有关于本合同事项的口头或书面的纪要、备忘录、协议和合同等法律文件。

11.3 本合同书一式 伍 份，甲方 叁 份，乙方 贰 份，自双方签字盖章之日起生效。

（以下无正文，为签字区）

甲方（盖章）：

授权代表人（签字）：于大洋

签订日期：2025.8.21

乙方（盖章）：

授权代表人（签字）：徐明

签订日期：2025.8.21

附件 1：云资源使用

（一）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。

（二）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、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。

（三）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，a 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。

（四）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 2：信息系统售后服务及数据接口对接、模块升级

（一）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。

（二）**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。

（三）系统运维：设固定专职常驻客服人员 1 人，另在甲方办公地点设运维常驻人员不少于 2 人，跟踪负责解决客户的所有问题。以上专员需熟悉医院相关工作，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，并反馈至信息中心
	报表、表单修改类	2 天内分配	5 天内处理完毕，并反馈至信息中心
	数据修改提取、对账类	2 天内分配	7 天内处理完毕，并反馈至信息中心
	故障排查类（针对软件类）	1 天内分配	5 天内处理完毕，并反馈信息中心排查结果
	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

（四）接口服务：乙方为甲方提供现行第三方信息系统及后续第三方信息系统的长期对接。

（五）医院信息系统模块（附系统清单）版本架构内的补丁升级，BUG 修复，性能优化提升等。

序号	名称
1.	预约系统
2.	档案浏览器系统
3.	入院准备中心信息系统
4.	高值耗材管理系统
5.	门诊电子病历系统

6.	分诊叫号系统
7.	医疗质量控制系统
8.	康复管理系统
9.	慢病管控平台
10.	产房系统
11.	血糖管理系统
12.	移动护士端系统
13.	医保核心服务
14.	医保结算清单系统
15.	移动医生端系统
16.	患者智慧服务系统
17.	医保结算清单质控
18.	临床智慧大屏系统
19.	一体化办公平台(电脑版)
20.	移动版 OA
21.	对账平台
22.	健康报表平台
23.	健康数据中心
24.	电子病历系统
25.	单病种质控系统
26.	VTE 系统
27.	手术麻醉系统
28.	血液透析管理系统
29.	HIS 系统
30.	病案信息管理系统
31.	血液管理信息系统
32.	心电网络系统
33.	数字病理信息系统
34.	危急值闭环管理系统
35.	重症监护系统
36.	病案首页质量控制系统
37.	急诊系统
38.	医师医保管理助手
39.	医院感染实时监控系统
40.	DIP 运营监测系统
41.	公共卫生上报系统
42.	供应室追溯系统

43.	院长管控平台
44.	PACS 系统
45.	医务管控平台
46.	临床路径管理系统
47.	科主任管控平台
48.	体检管理系统
49.	智慧质控系统
50.	电子病历归档系统
51.	护理文书系统
52.	三维重建系统
53.	合理用药系统
54.	医疗影像辅助诊断系统
55.	数据服务接口平台
56.	LIS 系统
57.	智慧护理管理系统
58.	门诊输液系统
59.	随访管理系统
60.	静脉配置中心系统
61.	医保办管理系统
62.	门诊管控系统
63.	创伤中心
64.	卒中中心
65.	胸痛中心
66.	门急诊诊疗信息页管理系统

三、其他要求：

（一）服务方案要求：供应商应针对本项目出具完善服务方案，包括

1.基础服务、预防性服务、其他服务：供应商需为本项目提供基础服务、预防性服务、其他服务。

2.服务响应体系的服务标准、服务方式、服务回访：供应商需具备完善的服务响应体系，说明服务响应体系的服务标准、服务方式、服务回访。

3.服务措施：供应商需提供 7*24 小时技术服务支持，包括提供远程支援、电话咨询和现场技术处理等服务。

（二）安全保障方案要求：

供应商需在保障现有系统安全体系的前提下，提出确保软件安全可靠的安全策略、安全措施及安全步骤，要求内容全面、符合采购人的实际情况。

（三）应急方案要求：

供应商应针对本项目出具完善应急方案，包括

1.保障措施或应急预案：供应商需具备完整的保障措施或应急预案，针对项目可能出

现的应急情况提出具体保障措施，保障业务应用的安全稳定运行。

2. 应急人员配备情况：供应商需提供拟投入本项目的应急人员名单，应急人员需配备齐全、分工明确。

（四）保密方案要求：

供应商应针对本项目出具完善保密方案，包括

1. 人员管理制度：供应商需具备完善的人员管理制度。

2. 保密措施：供应商需具备完整的保密措施。

（五）人员团队配备方案要求：

供应商应针对本项目出具完善人员团队配备方案，包括

1. 项目组织结构：供应商需具备完善的项目组织结构。

2. 人员的专业水平：供应商需提供相关证明材料，证明服务人员的专业水平。

3. 项目内部管理制度：供应商需具备完整的项目内部管理制度。

（六）运维方案要求：供应商需拥有统一的运维管理平台，具备全面的授权管理机制、完善的生产环境审计机制。

（七）服务期内，供应商需实现远程网络维护，作为现场维护的补充。