

(服务类)

## 信息系统建设服务合同

项目名称：北京友谊医院顺义院区应用系统与研究所  
信息化建设项目（医院部分）招标

甲方：首都医科大学附属北京友谊医院

乙方：北京移动系统集成有限公司



甲方：首都医科大学附属北京友谊医院

地址：北京市西城区永安路 95 号

联系人： 刘志军

联系电话： 63139390

乙方： 北京移动系统集成有限公司

地址： 北京市东城区东直门南大街 7 号 9 层 2 室

联系人： 单译葳

联系电话： 13810202495

甲方就 北京友谊医院顺义院区应用系统与研究所信息化建设项目（医院部分） 招标（项目名称）中所需 物联网应用开放平台（信息系统名称）经 中技国际招标有限公司（招标代理机构）以 0701-254106140767 号招标文件在国内 北京市 招标。经评标委员会评定乙方为中标人。甲乙双方同意按照下面的条款和条件，签署本合同。

## 第一条 服务信息

1、乙方向甲方提供信息系统建设服务的名称为：物联网应用开放平台（以下简称“本项目”）。

2、本项目的价款为人民币 595000 元（大写：人民币伍拾玖万伍仟元整）。合同价款包括但不限于信息系统开发费用、税金、包装、运输、保险、安装调试、培训费、根据法律法规应由乙方承担的税款等本合同项下甲方需向乙方支付的全部费用，除此之外，甲方无需因本合同向乙方支付任何费用。

3、本项目的服务内容详见附件一《信息系统功能需求清单》、附件二《售后服务方案》、附件三《运维服务方案》、附件四《中标通知书》，为本合同不可分割的一部分，与本合同具有同等法律效力。

## 第二条 乙方主体资格

1、乙方应向甲方提供签订本合同所需的全部资质文件的复印件，在复印件上注明与原件一致并加盖公章。

2、本合同项下，乙方应向甲方提供的乙方的资质文件为：

☒营业执照；

☐软件产品登记表；

☐软件著作权登记证书；

☐专利证书；

☐系统集成企业资质登记证明；

☐营销人员授权书；

☒售后服务承诺书；

☐产品代理授权书；

☐其他：\_\_\_\_\_ / \_\_\_\_\_。

### 第三条 付款方式

1、甲方根据北京市财政支付流程向乙方支付合同总价款，合计为人民币595000元整（大写：人民币伍拾玖万伍仟元整）

根据北京市财政资金拨付进度，第一期款项不低于合同总价款的60%，此后，甲方根据北京市财政资金到账情况，向乙方支付合同款项。

甲方收到货物并验收合格前，甲方有权不向乙方支付全额款项。

2、甲方每次付款前，乙方应向甲方提供符合甲方要求的发票，甲方确认发票内容及金额无误后，向乙方支付款项。乙方未提供发票，或者提供发票的内容或金额有误的，甲方有权拒绝支付相应款项且无需承担任何违约责任。

3、乙方账户信息如下：

账户名称： 北京移动系统集成有限公司

开户行： 上海浦东发展银行北京分行营业部

银行账号： 91010078801600000291

4、甲方开票信息如下：

账户名称：首都医科大学附属北京友谊医院

开户行名称：工商银行珠市口支行营业室

开户行账号：0200003109089210458

纳税人识别号：121100004006886096

5、本合同项下支付及结算（☒适用/☐不适用）财政资金支付程序。如本合同项下的支付及结算适用财政资金支付程序的，则以财政资金的支付及结算程序为准，与之相抵触的约定无效。

#### 第四条 甲乙双方的权利及义务

1、甲方的权利及义务如下：

（1）甲方指定专人负责在本合同执行过程中的组织和协调工作。

（2）甲方按需组织协调解决问题，跟踪工作进度。

（3）甲方为乙方现场安装调试和正式部署提供必要的软件、硬件、网络、基础数据等条件，以满足软件安装调试的需要。

（4）为使本项目完成后能更好地进行今后的维护工作，甲方安排一名以上维护人员全程跟踪学习、参与安装调试。

（5）甲方有权知晓各种技术和方案的细节，并提出改进意见。

（6）在任何时候，甲方对乙方负责本项目的专业人员的主要工作表现不满意，可立即书面告知乙方，并可要求乙方更换人员。乙方应采取合理措施，在收到甲方的书面告知后 10 个工作日内予以解决。

（7）乙方（☒需要/☐不需要）向甲方提供源代码。乙方如须要向甲方提供源代码的，甲方应保证源代码的使用仅限于内部进行系统维护使用，未经乙方许可，甲方不得将源代码及修改后的源代码提供给任何第三方。

（8）乙方提供的软件（☒需要/☐不需要）与甲方院内其他系统进行接口。如须要与甲方院内其他系统进行接口的，甲方应负责参与协调接口协议和参与拟定数据标准。

（9）甲方负责及时签收乙方交付的软件及相关产品，按本合同约定进行验收，并按照本合同规定的付款方式及时付款。

（10）其他：\_\_\_\_\_ / \_\_\_\_\_

2、乙方的权利及义务如下：

（1）乙方指定 李冉 为乙方的联系人，协调履行本合同的权利和履行义务。乙方联系人的联系电话为： 13910256571 。

(2) 以下条件符合后,乙方应在1个月内完成安装调试、测试、人员培训等系统上线工作,待甲方验收合格后交付甲方正式使用:

☐本合同签订后\_\_\_\_/\_\_\_\_内

☒乙方收到甲方根据支付的第一笔合同款项后15日\_\_\_\_内

☐其他:\_\_\_\_/\_\_\_\_

(3) 乙方向甲方派遣适合本合同要求的技术人员队伍,并指派专人负责该工作,确保按双方约定的要求保质、保量地完成本项目的开发安装调试工作。

(4) 乙方交付的技术服务工作成果应满足网络安全等级保护3级基本要求,并服务过程中或在维保期内需无偿向甲方提供对安全漏洞的修复服务。

(5) 乙方(☒需要/☐不需要)提供本项目中所含的客户端正版操作系统。

(6) 乙方应按照以下约定,及时、主动地向甲方提交书面工作报告,告知工作进展及所须要解决的问题:

☐每日

☐每周

☒其他:\_\_\_\_以甲方要求为准\_\_\_\_

(7) 乙方应指导甲方相关人员进行基础数据的准备、整理工作。

(8) 在整个安装调试过程中,乙方应对甲方相关人员进行软件功能、作用、和使用操作等培训。

(9) 乙方应向甲方提供甲方要求的、不涉及乙方保密信息的所有文档及技术资料。

(10) 如因乙方原因无法为甲方提供持续的售后服务和产品升级,乙方(☒需要/☐不需要)无偿向甲方提供以下资料,以保证甲方系统的正常稳定运行:

☒源代码;

☒运维手册;

☒数据结构;

☐其他:\_\_\_\_/\_\_\_\_

(11) 乙方应根据本合同的相关条款及甲方的要求,对系统提供质保和维修。乙方应保障系统不发生重大故障,否则甲方有权追究乙方相关责任。

(12) 未经甲方事先书面同意,乙方不得将本项目涉及的软硬件系统、数据库、数据、影像等内容进行任何加密设置,不得对甲方应用本项目相关的系统和

数据设置任何限制。如乙方认为必须进行加密的，必须事先取得甲方的书面同意，并向甲方提供解密算法。

(13) 其他：\_\_\_\_\_ / \_\_\_\_\_

第五条 售后服务条款及质保服务

1、本项目自验收之日起  3  年内为质保期，乙方应提供免费维护服务。

2、质保期内，乙方应向甲方提供如下质保服务：

(1) 乙方提供 (☒7\*24 小时/☐5\*8 小时/☐其他：  /  ) 技术支持，并不限支持次数。乙方应根据以下的故障等级提供相应的处理：

| 故障等级 | 故障等级定义                                                        | 处理时间及方式                                                                                                                                                                                                             |
|------|---------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 一级故障 | 系统瘫痪、严重影响系统使用、严重影响其他关键业务正常使用，如：系统无法访问、数据库无法连接等                | 立即响应，( <input checked="" type="checkbox"/> 1 小时内/ <input type="checkbox"/> _/_ 小时内) 电话/网络远程支持，并通过最快交通方式到达故障现场，到达现场后 4 小时内解决故障（因特殊原因无法在 4 小时内解决故障的，经甲方同意后可适当延长）。                                                     |
| 二级故障 | 影响系统使用、影响其他关键业务正常使用，如：系统能正常访问，但部分功能模块无法使用。                    | 立即响应，( <input checked="" type="checkbox"/> 2 小时内/ <input type="checkbox"/> _/_ 小时内) 电话/网络远程支持，12 小时内到达故障现场。到达现场后 4 小时内解决故障（因特殊原因无法在 4 小时内解决故障的，经甲方同意后可适当延长）。                                                        |
| 三级故障 | 轻微影响使用，远程支持后可解决；不影响其他关键业务使用，如：系统自身的 BUG，甲方对系统使用的疑问，对系统新功能的咨询等 | ( <input checked="" type="checkbox"/> 30 分钟内/ <input type="checkbox"/> _/_ 小时内) 响应，( <input checked="" type="checkbox"/> 2 小时内/ <input type="checkbox"/> _/_ 小时内) 内电话/网络远程支持并解决故障（因特殊原因无法在 2 小时内解决故障的，经甲方同意后可适当延长）。 |

(2) 乙方 (☐需要/☒不需要) 免费为甲方技术人员进行系统管理、操作培训，培训次数不得少于  /  次，具体次数由甲方指定。

(3) 乙方提供专门技术服务人员进行项目后期跟踪，提供每年不少于  1  次的 (☐现场/☒非现场) 服务，及时检查并处理问题。

4、质保期满后，乙方（☒需要/☐不需要）提供常年维保服务。如乙方须要提供常年维保服务的，甲乙双方应另行签订维保服务协议，每年维护费用为：

□人民币 / 元 (大写: 人民币 / )

5、乙方 (☒需要/☐不需要) 向甲方提供本合同中所有系统模块的维护、功能和代码的优化。

1、本项目满足附件一《信息系统功能需求清单》，系统上线稳定运行1个月，且甲方相关使用部门签字确认后，由乙方提出书面验收申请。甲方收到乙方的验收申请后，对系统的整个情况进行评估验收。乙方应确保系统的全部有关技术文件、资料、及安装、测试、验收报告等文档完整交付。验收合格后，甲方签署验收报告。验收不合格甲方需书面告知乙方不合格原因，乙方负责按照验收标准整改并再次提出验收申请，直到验收合格。

□其他: \_\_\_\_\_ / \_\_\_\_\_

CON202509050

目验收。

## **第七条 知识产权**

1、乙方保证甲方及其用户在使用本合同项下产品、服务及其任何部分时，不会受到任何第三方关于侵犯专利权、商标权、工业设计权或知识产权的质疑。任何第三方如果提出侵权质疑，乙方须与第三方交涉并承担可能发生的一切法律责任和费用。

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

3、在本合同有效期内，乙方利用甲方提供的知识类资料所完成的知识类成果，归甲方所有。

4、由各方各自独立开发的专利以及其他知识产权归属各自所有。

## **第八条 保密**

保密信息是指甲乙双方各自专有的、或提供给对方的并明确标有“保密”字样的信息，包括但不限于本合同及其签订、许可软件、数据等。甲乙双方承认保密信息构成有价值的商业秘密。甲乙双方同意严格按照本合同的规定使用对方的保密信息，未经对方的事先书面许可，不得向第三方，或允许向第三方直接或间接地透露保密信息。本合同的保密义务为永久。无论本合同变更、解除或终止，本条款保持有效。

## **第九条 违约责任**

1、乙方应按本合同约定完成本项目的服务工作，乙方每延迟一日，需支付合同总价款 1%的违约金。延迟交付达 15 日的，甲方有权单方解除本合同，要求乙方返还甲方已支付的合同价款，并承担相当于合同总价款 20%违约金。若因归责于甲方原因导致延迟，或乙方因特殊原因导致延迟且事前取得甲方书面同意的，乙方不承担违约责任。

2、因乙方未按甲方的网络安全要求执行或实施服务，而造成甲方不良网络安全事件、经济损失、恶劣社会影响，每发生一次，乙方应向甲方支付与损失等

价的赔偿金，赔偿金额按每起事故不低于合同总款的 5% 计算。

3、乙方应确保所提供成果和技术服务的稳健性，因乙方在提供技术服务过程中的过失、疏忽或技术服务工作成果的缺陷，引发的信息系统故障或业务数据损失，而造成甲方经济损失、不良社会影响的，每发生一次，乙方应向甲方支付与损失等价的赔偿金，赔偿金额按每起事故不低于合同总款的 5% 计算，同时乙方须按甲方要求积极负责排查故障原因，彻底解决问题。

4、乙方未能在本合同规定时间内到达现场或解决故障的，每延迟 4 小时，需支付合同总价款 1% 的违约金。但因特殊情况，甲方同意适当延长故障解决时间的除外。

5、乙方在接到甲方的维修要求后 24 小时内未能解决故障的，甲方有权指定第三方提供服务，由此造成的额外费用及给甲方造成的损失均由乙方承担。

6、乙方出现违约 3 次以上（含 3 次）的，或者延迟时间累积 24 小时（含 24 小时）时，甲方有权单方解除本合同，并要求乙方支付相当于本合同总价款 20% 的违约金。

7、乙方违反保密义务，造成甲方损失的，应支付甲方与泄密内容和不良影响等价的赔偿金，赔偿金额按每起事故不低于合同总款的 60% 计算。

8、违约金不足以弥补甲方因此遭受的损失，乙方还需就不足部分承担赔偿责任。

9、甲方有权从剩余应向乙方支付的款项中优先扣减乙方应向甲方支付的款项（包括但不限于违约金、赔偿金等）。

10、乙方未按本合同约定提供服务的，甲方有权要求乙方延长免费维护期。延长的免费维护期限由甲方决定。如乙方对甲方提出的维护期限有异议的，应提出书面异议并说明理由。乙方提出书面异议的，甲乙双方通过协商决定延长的免费维护期限的时长，但该免费维护期限不得低于乙方未按照本合同约定提供服务的合计时长。

## **第十条：信息集成**

乙方应确保所提供成果和技术服务满足甲方的信息集成要求：

1、业务字典需通过甲方信息集成平台与主数据系统对接；

- 2、业务数据要求需按照甲方标准接口定义通过信息集成平台进行对接；
- 3、信息系统中业务数据需根据甲方需求，支持但不限于数据库同步、视图、接口等集成方式开放；
- 4、支持 HL7 V3、HL7 FHIR 等国家或行业标准，以及甲方自定义标准接口对接；
- 5、支持各类传输访问协议，包括但不限于 HTTP/HTTPS、TCP/IP、SFTP、SOAP/HTTP；
- 6、支持满足安全要求的数据存储及传输的加密/解密；
- 7、支持根据甲方需要的数据或业务功能提供符合需求的 API 服务；
- 8、需按照甲方需求与其它信息系统进行表示、数据、控制、业务流程等方式的集成。

#### **第十一条 国产化适配要求**

乙方应按甲方要求配合进行国产化适配和替代，以确保所提供的信息系统能够在国产操作系统、国产数据库、国产中间件等国产基础软件环境中运行和使用，所有功能保持一致，性能确保稳定，包括服务端。

#### **第十二条 系统兼容要求**

乙方应确保所提供的信息系统或主要设备能够兼容 Windows7 及以上版本，所有功能和性能保持一致、稳定。

#### **第十三条 不可抗力**

因自然灾害、战争、政府指令、政府主权行为、法律变化等不可预见、不可避免、不可克服的不可抗力事件导致本合同一方当事人无法履行本合同的，受不可抗力事件影响的一方不承担违约责任，但遭受不可抗力一方因延迟履行本合同义务后遭遇的不可抗力事件除外。受到不可抗力事件影响的一方应采取措施将不可抗力事件的负面影响降到最低，否则应对对方当事人的损失扩大部分承担赔偿责任。受到不可抗力事件影响的一方应在不可抗力发生后 2 日内书面通知对方当事人，并在不可抗力发生后 5 个工作日内向对方当事人出示不可抗力发生地有权部门出具的不可抗力事件的证明。没有在约定时间内通知对方当事人，给对方当

事人造成损失的，负有通知义务的一方应承担相应的赔偿责任。

#### **第十四条 权利义务的转让**

未经甲方事前书面同意，乙方不得将其基于本合同的权利义务的全部或者部分向第三人转让，也不得用以提供担保。

#### **第十五条 合同变更及终止**

1、乙方发生以下各项的任何一种情形的，甲方无需催告等其他手续，可直接解除全部或者部分本合同。

- (1) 开具的票据或者支票不能承兑，或者陷于停止支付、不能支付的；
- (2) 受到监督机构停止营业或者吊销营业执照等处分的；
- (3) 申请或者被申请破产、清算、拍卖等任何一种手续及与其类似的其他手续；
- (4) 被第三人申请财产保全、强制执行、申请拍卖或者受到其他公权力处分；
- (5) 作出解散决议的；
- (6) 由于灾害、劳动争议或者其他原因，导致本合同履行困难；
- (7) 发生类似前述各项导致经营困难的事由的。

2、甲乙双方可以在取得对方书面同意的情况下，解除本合同或变更本合同。

#### **第十六条 争议解决**

因本合同产生的所有争议，甲乙双方应本着诚意友好协商解决。协商无法解决时，任何一方有权向甲方所在地有管辖权的人民法院起诉。

#### **第十七条 合同文件**

下列文件构成本合同的组成部分，应该认为是一个整体，彼此相互解释，相互补充。为便于解释，组成合同的多个文件的优先支配地位的次序如下：

- a. 本合同书
- b. 中标通知书

c. 招标文件（含招标文件补充通知）

d. 投标文件（含澄清文件）

### **第十八条 廉洁条款**

1、甲方人员不得向乙方索要且乙方不得向甲方人员或其家属提供任何酬金、礼物或其它有形或无形之利益，上述行为应被视为商业贿赂，一经发现并查实，双方当事人将受到相应的法纪、政纪处理；同时，甲方有权停止与乙方之后的所有业务合作。

### **第十九条 其他**

1、本合同经甲乙双方的法定代表或授权代表签字并加盖公章后生效。

2、本合同未尽事宜，甲乙双方协商一致后签订书面补充协议。补充协议作为本合同的一部分，与本合同具有同等法律效力。

3、本合同一式六份，甲方执四份，乙方执二份，各份具有同等法律效力。

(本页为签字页，无正文)

甲方：首都医科大学附属北京友谊医院  
(盖章)



法定代表人或授权代表

(签字)：

日期：20 18 年 9 月 22 日

乙方：北京移动系统集成有限公司  
(盖章)



法定代表人或授权代表

(签字)：

日期：20 18 年 9 月 22 日

附件一：《信息系统功能需求清单》

| 序号 | 服务内容                            |           | 服务期限         |
|----|---------------------------------|-----------|--------------|
| 1  | 物联网应用开<br>放平台（功能<br>升级扩展服<br>务） | 接入适配功能    | 自合同签订之日起 4 年 |
|    |                                 | 设备管理功能    |              |
|    |                                 | 数据可视化功能   |              |
|    |                                 | 数字集成功能    |              |
|    |                                 | 设备及账户升级管理 |              |
| 2  | 方案设计与项目管理                       |           |              |

## 附件二：《售后服务方案》

### 1.1. 售后服务方案

#### 1.1.1. 服务内容

##### （一）日常运维支持

平台监控：远程支撑客户开展对物联网平台的监控，包括服务器运行状态、网络连接状况、设备接入情况、数据传输情况等，及时发现并处理潜在问题，确保平台持续稳定运行。

系统巡检：定期对平台进行全面巡检，包含常规巡检和深度巡检。常规巡检内容包括平台各项功能模块的运行情况、设备在线率、数据准确性等；深度巡检内容涵盖系统架构、数据库性能、安全漏洞等方面，形成详细的巡检报告并及时反馈给客户。

数据维护：负责平台数据的日常维护工作，包括数据备份、数据清理、数据恢复等。按照客户要求定期进行数据备份，确保数据的安全性和完整性。同时，对冗余数据进行清理，优化数据库性能。

设备维护支持：为接入平台的各类设备提供维护支持，包括智能体温贴、血压仪、体征监测仪、智能床垫、智能感知等设备。协助客户进行设备故障排查、设备参数调整等工作，提供技术指导和解决方案。

##### （二）技术支持服务

咨询服务：设立专门的技术咨询热线和邮箱，为客户提供技术咨询服务。解答客户在平台使用过程中遇到的各类技术问题，包括平台功能操作、设备接入配置、数据查询分析等。

培训服务：在平台验收后，为客户提供全面的技术培训服务。培训内容包括平台的基本操作、设备管理、数据可视化分析、系统配置等方面。根据客户需求，制定个性化的培训方案，确保客户相关人员能够熟练使用平台，培训次数不少于 2 次。

##### （三）问题解决服务

故障排除：接到客户的故障报告后，迅速组织技术人员进行故障排查和处理。对于一般性故障，在规定时间内解决；对于复杂故障，成立专项技术小组进行攻

关，制定解决方案并尽快实施，确保平台恢复正常运行。

需求响应：针对客户在平台使用过程中提出的新需求和功能优化建议，及时进行评估和反馈。对于合理的需求，纳入平台升级计划或提供定制化解决方案；对于暂时无法实现的需求，向客户说明原因并提供替代方案。

### 1.1.2. 故障响应

#### （一）响应机制

建立完善的故障响应机制，设立专门的故障响应中心，配备专业的技术人员和先进的故障监测设备。客户可通过电话、邮箱、在线平台等多种渠道报告故障，故障响应中心接到报告后，立即进行登记和分类处理。

#### （二）响应时间

紧急故障：指平台核心功能失效、大面积设备离线、数据丢失等严重影响平台运行的故障。接到故障报告后，技术人员在 2 小时内提供技术响应。

一般故障：指平台个别功能操作不便、数据显示异常等对平台运行影响较小的故障。接到故障报告后，技术人员在 8—24 小时之内提供技术响应。

#### （三）故障处理流程

故障受理：故障响应中心接到客户故障报告后，详细记录故障现象、发生时间、影响范围等信息，并进行初步判断和分类。

故障诊断：技术人员根据故障信息进行深入诊断，确定故障原因和解决方案。如需要现场排查，及时安排技术人员前往现场。

故障处理：按照解决方案进行故障处理，在处理过程中及时向客户反馈进展情况。处理完成后，对故障进行验证，确保故障已彻底解决。

故障总结：故障解决后，对故障原因、处理过程和结果进行总结，形成故障处理报告，为后续的平台维护和优化提供参考。

### 1.1.3. 应急处理措施

#### （一）应急团队组建

成立应急处理专项团队，由项目经理、技术负责人、资深开发工程师、运维工程师等组成。应急团队成员具备丰富的物联网平台应急处理经验，能够在紧急情况下迅速响应和处理问题。

#### （二）应急预案制定

针对可能出现的重大故障和突发事件，制定详细的应急预案，包括服务器宕机、网络中断、数据泄露、大规模设备故障等场景。应急预案明确应急处理流程、责任分工、资源调配等内容，并定期进行演练和优化。

### （三）应急处理流程

突发事件发生后，应急团队迅速启动应急预案，各成员按照职责分工开展工作。

技术人员立即对事件进行评估，确定事件的严重程度和影响范围，采取相应的控制措施，防止事态扩大。

组织技术力量进行问题排查和处理，尽快恢复平台的正常运行。在处理过程中，及时向客户和相关部门汇报进展情况。

事件处理完成后，对事件进行全面复盘，分析原因，总结经验教训，完善应急预案和平台安全措施。

### （四）数据安全应急措施

**数据备份与恢复：**定期对平台数据进行备份，建立多副本备份机制，确保数据在发生丢失或损坏时能够及时恢复。备份数据存储在安全可靠的位置，并进行加密处理。

**数据泄露应急处理：**如发生数据泄露事件，立即启动数据泄露应急预案，封锁相关数据访问通道，排查泄露原因，采取措施防止数据进一步泄露。同时，及时向客户和相关部门报告，配合进行调查和处理。

## 1.1.4. 服务保障措施

### （一）服务质量保障

建立服务质量监督机制，设立服务质量监督小组，定期对售后服务工作进行检查和评估。通过客户满意度调查、服务质量考核等方式，不断提高服务质量。

制定服务质量标准和规范，明确服务人员的职责和行为准则，确保服务过程的规范化和标准化。对服务人员进行定期培训和考核，提高服务人员的专业素质和服务意识。

### （二）资源保障

**技术资源：**投入充足的技术资源，包括专业的技术人员、先进的技术设备和软件工具等，确保能够为客户提供高质量的售后服务。

备件资源：建立备件库，储备平台运行所需的各类备件和设备，如服务器配件、网络设备、传感器等，确保在设备出现故障时能够及时更换。

信息资源：建立完善的信息管理系统，对客户信息、设备信息、故障处理记录等进行统一管理，为售后服务提供准确的信息支持。

### （三）沟通协调保障

建立定期沟通机制，每月与客户进行一次沟通会议，汇报平台运行情况、售后服务工作进展等，听取客户的意见和建议，及时解决客户提出的问题。

加强内部沟通协调，建立售后服务工作群，确保各部门之间信息畅通，协同配合完成售后服务工作。对于复杂问题，及时组织内部讨论，制定解决方案。

#### 1.1.5. 维护人员配置

##### （一）维护团队组成

运维主管：具备丰富的物联网平台运维管理经验，负责维护团队的日常管理工作，制定运维计划和方案，协调解决重大运维问题。

运维工程师：熟悉物联网平台的架构和运行机制，负责平台的日常监控、巡检、故障处理等工作，提供技术支持和服务。

开发工程师：具备物联网平台开发经验，负责平台的版本升级、功能优化、定制化开发等工作，协助解决技术难题。

技术支持专员：负责客户的技术咨询、故障报告受理、服务协调等工作，确保客户需求得到及时响应和处理。

##### （二）人员职责与分工

运维主管：全面负责售后服务工作的规划、组织、协调和监督；制定运维管理制度和流程；审核运维计划和方案；协调解决重大故障和客户投诉；定期向公司和客户汇报售后服务工作情况。

运维工程师：负责平台的日常监控和巡检，及时发现和处理平台故障；进行数据备份、清理和恢复等工作；协助客户进行设备维护和管理；提供技术支持和培训服务。

开发工程师：负责平台的版本升级和功能优化；根据客户需求进行定制化开发；解决平台开发过程中的技术问题；协助运维工程师进行故障排查和处理。

技术支持专员：负责接听客户咨询电话和处理客户邮件；受理客户故障报告

并进行登记和分类；协调技术人员为客户提供服务；跟踪故障处理进展情况并及时向客户反馈；进行客户满意度调查和服务质量评估。

### （三）人员资质要求

维护团队成员需具备相关的专业知识和技能，持有相关的职业资格证书，如计算机技术与软件专业技术资格证书等。同时，具备良好的沟通能力、团队协作能力和问题解决能力，能够为客户提供优质的售后服务。

## 附件三：《运维服务方案》

### 1.2. 实施方案

#### 1.2.1. 项目管理

本项目将采用科学、规范的项目管理方法，确保顺义院区物联网平台建设项目顺利实施。建立以项目经理为核心的项目管理团队，明确各成员的职责与分工。

##### （一）项目组织架构

设立项目经理、技术负责人、开发工程师、测试工程师、实施工程师、运维工程师等岗位。项目经理全面负责项目的整体规划、协调与把控；技术负责人专注于技术方案的制定、技术难题的攻克以及技术团队的管理；开发工程师承担平台功能的开发工作；测试工程师负责对平台进行全面测试，保障平台质量；实施工程师负责平台的安装、部署与调试；运维工程师则在项目完成后提供持续的运维支持。

##### （二）项目管理流程

**需求分析与确认：**深入理解客户的技术需求，组织与客户的沟通会议，对需求进行详细分析和确认，形成需求规格说明书，经双方签字确认后作为项目开发的依据。

**计划制定：**根据需求规格说明书，制定项目的整体计划，包括项目范围、进度、成本、质量等方面的计划，并明确各阶段的里程碑。

**开发与测试：**按照计划开展平台的开发工作，采用迭代开发的方式，每完成一个迭代周期，及时进行内部测试，发现问题及时修复。

**实施与验收：**完成平台开发和测试后，进行平台的安装、部署与调试，组织客户进行验收。验收通过后，项目进入运维阶段。

**沟通与协调：**建立定期的沟通机制，包括项目例会、周报、月报等，及时向客户汇报项目进展情况，解决项目中出现的问题。同时，加强团队内部的沟通与协调，确保各项工作有序推进。

#### 1.2.2. 建设计划与进度方案

##### （一）项目阶段划分

本项目分为需求分析与设计阶段、开发阶段、测试阶段、安装调试阶段、系统联调阶段、验收阶段以及运维阶段。

## （二）各阶段进度安排

需求分析与设计阶段（第 1 周）：与客户进行深入沟通，明确项目需求，完成平台的架构设计、数据库设计、功能模块设计等工作，并形成设计文档，提交客户确认。

开发阶段（第 2-3 周）：根据设计文档开展平台的开发工作，包括接入适配功能、设备管理功能、数据可视化功能、数字集成功能以及设备及账号管理升级等模块的开发。每周进行一次开发进度检查，确保开发工作按计划进行。

测试阶段（第 2-3 周）：对开发完成的平台进行全面测试，包括功能测试、性能测试、安全测试等。测试过程中发现的问题及时反馈给开发团队进行修复，直至平台满足需求规格说明书的要求。

安装调试阶段（第 4 周）：将平台安装部署到客户指定的环境中，进行设备的接入调试、系统配置等工作，确保平台能够正常运行。

系统联调阶段（第 4 周）：与医院现有的业务系统进行联调，实现数据的互联互通，验证平台与其他系统的兼容性和稳定性。

验收阶段（第 9 周）：组织客户对平台进行验收，提交验收报告。若验收不通过，根据客户提出的问题进行整改，直至验收通过。

运维阶段（项目验收后 1 年）：提供持续的运维支持，包括平台的日常监控、故障处理、性能优化等工作，确保平台的稳定运行。

### 1.2.3. 实施人员安排

#### （一）项目核心团队

项目经理（1 名）：具备丰富的物联网平台项目管理经验，熟悉项目管理流程和方法，能够有效协调各方资源，确保项目顺利实施。

技术负责人（1 名）：拥有深厚的物联网技术功底，熟悉物联网平台的架构设计和开发技术，能够解决项目中的技术难题。

产品工程师（2 名）：拥有扎实的物联网平台产品开发经验，具备需求分析、原型设计等工作技能，确保产品能够满足客户需求。

开发工程师（3 名）：精通 Java、Python 等开发语言，具备物联网平台开发经验，负责平台各功能模块的开发工作。

测试工程师（1 名）：熟悉软件测试流程和方法，具备丰富的测试经验，负

责平台的测试工作，保障平台质量。

实施工程师（2名）：具备物联网平台安装、部署和调试经验，负责平台的现场实施工作。

运维工程师（1名）：熟悉平台的运维工作，负责平台的日常监控、故障处理等工作。

## （二）人员职责与分工

明确各人员在项目各阶段的职责与分工，确保各项工作有人负责、有人跟进。项目经理负责项目的整体协调与管理；技术负责人负责技术方案的制定和技术难题的解决；产品工程师负责平台产品设计工作；开发工程师负责平台的开发工作；测试工程师负责平台的测试工作；实施工程师负责平台的安装、部署和调试；运维工程师负责平台的运维支持。

### 1.2.4. 安全保障措施

#### （一）数据安全保障

数据加密：对平台中的敏感数据进行加密处理，包括设备数据、用户信息等，采用先进的加密算法，确保数据在传输和存储过程中的安全性。

访问控制：建立严格的访问控制机制，对用户进行身份认证和授权管理，不同角色的用户拥有不同的操作权限，防止未授权人员访问和操作数据。

数据备份与恢复：定期对平台的数据进行备份，建立数据备份策略，确保数据在发生意外丢失时能够及时恢复。同时，对备份数据进行加密存储，防止数据泄露。

#### （二）系统安全保障

网络安全：采用防火墙、入侵检测系统等网络安全设备，加强网络边界防护，防止网络攻击和非法入侵。定期对网络安全设备进行配置更新和漏洞扫描，确保网络安全。

系统漏洞管理：建立系统漏洞管理机制，定期对平台进行漏洞扫描和评估，及时发现和修复系统漏洞，降低系统安全风险。

安全审计：对平台的操作行为进行安全审计，记录用户的登录、操作等行为，便于事后追溯和审计，发现异常行为及时处理。

#### （三）设备安全保障

设备身份认证：为接入平台的设备颁发唯一的设备 ID 和登录密钥，实现设备的身份认证，防止非法设备接入平台。

设备访问控制：对设备的访问进行控制，只有经过授权的设备才能与平台进行通信，防止设备被非法操控。

设备固件安全：加强设备固件的安全管理，对设备固件进行加密和签名，防止固件被篡改和恶意攻击。

#### 1.2.5. 安装调试

##### （一）安装前准备

环境检查：对客户的服务器环境、网络环境等进行检查，确保满足平台的安装要求。包括服务器的硬件配置、操作系统版本、数据库版本、网络带宽等。

设备清点：对平台所需的硬件设备、软件介质等进行清点，确保设备齐全、完好。

技术培训：对实施人员进行平台安装调试技术培训，使其熟悉安装流程和操作方法。

##### （二）安装过程

服务器部署：将平台的服务器端软件安装部署到客户指定的服务器上，包括应用服务器、数据库服务器等。

客户端安装：根据需要，为客户安装平台的客户端软件，确保客户端能够正常访问服务器。

系统配置：对平台进行系统配置，包括数据库连接配置、网络配置、安全配置等。

##### （三）调试过程

设备接入调试：对需要接入平台的设备进行调试，包括设备的注册、连接、数据传输等。确保设备能够正常接入平台，并准确上传数据。

功能调试：对平台的各项功能进行调试，包括接入适配功能、设备管理功能、数据可视化功能、数字集成功能等。验证功能是否符合需求规格说明书的要求。

性能调试：对平台的性能进行调试，包括并发处理能力、响应时间等。通过性能测试和优化，确保平台能够满足实际业务需求。

#### 1.2.6. 系统联调

### （一）联调准备

制定联调计划：明确联调的目标、范围、内容、方法和步骤，制定详细的联调计划。

准备联调环境：搭建与实际生产环境一致的联调环境，包括服务器环境、网络环境、数据库环境等。

准备测试数据：准备联调所需的测试数据，包括设备数据、业务数据等。确保测试数据的真实性和完整性。

### （二）联调过程

与业务系统对接：将平台与医院现有的业务系统进行对接，实现数据的互联互通。包括数据的导入导出、接口调用等。

功能验证：验证平台与业务系统对接后的各项功能是否正常，包括数据的同步更新、业务流程的顺畅运行等。

性能测试：对平台与业务系统联调后的性能进行测试，包括系统的并发处理能力、响应时间等。通过性能测试和优化，确保系统的稳定性和可靠性。

问题解决：在联调过程中发现的问题及时进行记录和反馈，组织技术人员进行分析和解决，确保联调工作顺利进行。

### （三）联调总结

联调完成后，对得住工作进行总结，形成联调报告。报告中包括联调的基本情况、测试结果、问题及解决情况等内容，为后续的验收工作提供依据。

## 1.2.7. 质量保证措施

### （一）质量管理体系

建立完善的质量管理体系，按照 ISO9001 质量管理标准进行项目管理。从需求分析、设计、开发、测试、实施到运维等各个环节进行质量控制，确保项目质量。

### （二）质量控制措施

需求评审：对需求规格说明书进行评审，确保需求的准确性、完整性和一致性。评审人员包括项目经理、技术负责人、开发工程师、测试工程师以及客户代表等。

设计评审：对平台的架构设计、数据库设计、功能模块设计等进行评审，确

保设计方案的合理性和可行性。

代码审查：开发工程师提交代码后，由技术负责人组织进行代码审查，检查代码的规范性、可读性、安全性等。

测试控制：建立严格的测试流程，包括单元测试、集成测试、系统测试等。测试工程师按照测试计划和测试用例进行测试，确保测试覆盖率达到 100%。

文档管理：加强项目文档的管理，包括需求规格说明书、设计文档、测试报告、用户手册等。确保文档的完整性、准确性和一致性。

### （三）质量考核机制

建立质量考核机制，将项目质量与团队成员的绩效考核挂钩。对在项目中表现优秀、为保证项目质量做出贡献的团队成员进行奖励；对因工作失误导致项目质量问题的团队成员进行处罚。

## 1.2.8. 项目风险控制

### （一）风险识别

对项目实施过程中可能出现的风险进行全面识别，主要包括需求变更风险、技术风险、进度风险、质量风险、人员风险等。

### （二）风险评估

对识别出的风险进行评估，分析风险发生的可能性和影响程度，确定风险等级。根据风险等级制定相应的风险应对策略。

### （三）风险应对

需求变更风险：建立需求变更管理流程，对需求变更进行严格的评估和审批。在项目实施过程中，加强与客户的沟通，及时了解客户需求的变化，避免需求变更对项目进度和质量造成较大影响。

技术风险：在项目前期进行充分的技术调研和论证，选择成熟、稳定的技术方案。加强技术团队的培训和学习，提高技术人员的技术水平，确保能够解决项目中出现的技术难题。

进度风险：制定详细的项目计划，合理安排各项工作的进度。加强项目进度的监控和管理，及时发现进度偏差，并采取相应的措施进行调整。定期召开项目进度会议，协调各方资源，确保项目按计划进行。

质量风险：建立完善的质量管理体系，加强对项目各环节的质量控制。严格

执行测试流程，确保平台质量。加强对团队成员的质量意识培训，提高团队成员的质量意识。

人员风险：合理安排团队成员的工作任务，避免人员过度疲劳。加强团队建设，提高团队凝聚力和稳定性。制定人员备份计划，确保在关键岗位人员出现变动时，项目能够正常进行。

#### （四）风险监控

在项目实施过程中，持续对风险进行监控和跟踪，及时发现新的风险，并对风险应对措施的有效性进行评估。根据风险监控结果，及时调整风险应对策略，确保项目顺利实施。

附件四：《中标通知书》



中技国际招标有限公司

CHINA INTERNATIONAL TENDERING LIMITED COMPANY

编号 Ref. No.: ITCYW-6

日期 Date: 2025 年 9 月 11 日

发件人 From: 马建

致：北京移动系统集成有限公司

北京友谊医院顺义院区应用系统与研究所信息化建设项目(医院  
部分) 招标

(招标编号：0701-254106140767)

中标通知书

关于标题项目，经评标委员会评审，并经采购人审批同意，兹通知贵单位在如下内容的  
招标采购中中标：

| 包号 | 品目号 | 标的名称      | 数量  | 中标金额<br>(人民币元) |
|----|-----|-----------|-----|----------------|
| 6  | 6-1 | 物联网应用开放平台 | 1 项 | 595,000.00     |

请贵单位于本通知书发出后 3 日内与采购人联系，在本通知发出后 30 日内签署采购合  
同，采购合同签署后将合同扫描件发送至邮箱：majian4@cgci.gt.cn，我司将在收到合同扫  
描件后 5 个工作日内将投标保证金原路退回。

采购单位：首都医科大学附属北京友谊医院

采购人联系电话：010—63138216

我公司地址：北京市丰台区西营街 1 号院通用时代中心 C 座 9 层

联系人：马建

联系电话：81168697

谢谢参与！



抄送：首都医科大学附属北京友谊医院

CON202509050