**柳州市工人医院防统方系统技术参数要求**

1. **项目背景**

我院现有的防统方系统已使用12年，软件版本低，运行卡顿，功能已不能满足《中华人民共和国网络安全法》、《信息安全等级保护管理办法 2.0》等法律法规的相关要求以及医院现有业务数据的防统方管理要求，为了满足医院业务的发展和安全监管的需求，现需采购一套新的防统方系统，保证“统方”监控的全面完整及准确性，帮助医院更好地防止商业目的“统方”管理。**二、项目建设总体要求**

2.1系统应符合安全、高效、人机友好的原则，提供更好的用户体验，提升系统操作的简易性，和数据交互能力；

2.2系统功能满足医院现有业务数据的防统方管理要求以及《中华人民共和国网络安全法》和《信息安全等级保护管理办法 2.0》等法律法规的相关要求；

2.3系统支持灵活配置与升级、能够灵活地部署和优化业务流程；

2.4 系统用户操作界面友好，用户操作简单直观，易于学习掌握；

2.5 系统支持多种主流数据库；

2.6系统具有良好的兼容性和适配性，支持虚拟服务器、国产信创服务器上运行，平台支持改造在国产信创电脑上运行；

2.7系统支持个性化定制，根据客户业务场景定制开发，高度匹配客户应用场景，提高使用的友好性与易用性；

2.8系统不限制客户端用户数、并发数、可通过扩展后台服务器动态增加性能；

2.9系统支持多个院区共用一个数据库，统一管理标准，支持跨院区信息互通。

三 、**系统安全要求**

3.1 系统从应用安全、数据库安全、网络安全、操作安全、平台安全等多个方面进行安全保障；

3.2 系统可保证统方数据的真实性和有效性；

3.3 系统支持权限分级管理和访问控制。

**四、系统功能及硬件要求**

**4.1软件技术参数**

4.1.1支持多院区分布部署及监控；（提供截图并加盖公章）

4.1.2系统应具备对应用程序、数据库访问者、访问者IP地址等统计功能，并形成相应的报告；

4.1.3系统部署时不需要更改医院现有网络结构、服务器相关配置，系统运行不得影响现有网络和业务的正常运行，系统应能独立完成审计数据采集，不得在现有服务器上安装可能带来风险的程序，工作时不影响数据库本身的运行与性能；

4.1.4 系统支持统方事件的及时告警，并可根据不同的安全级别采用不同实时告警响应方式；

4.1.5系统的时间可以和关键服务器中的数据库的时间进行同步，确保记录时间的一致性；

4.1.6支持加密方式的数据库连接信息分析；（提供截图并加盖公章）

4.1.7提供多种数据库类型监测能力，支持监测Oracle、MS-SQL、DB2、MYSQL、CACHE DB、POSTGRESQL和Sybase等主流医疗数据库和国产数据库，对以上数据库提供自动化评估、审计和保护功能；

4.1.8系统从业务流程角度入手，结合核心数据特征，形成高度集成的“事前+事中+事后”数据防护手段；

4.1.9采用B/S架构（兼容不同种类浏览器），提供中文WEB管理界面以便于管理，并应可以根据不同的安全级别采用不同的实时告警响应方式，包括记录、消息、邮件等，并能支持短信平台；

4.1.10审计数据保存期限、存储方式、管理方式符合防统方管理要求；

4.1.11能够出具针对纪委、纪检监察室等相关人员使用的防统方审计报告，报告需简单明了，且具有主动将所有的计算机语言翻译成通俗易懂的自然语言的系统机制，支持将整条SQL语句翻译成中文，帮助医院建立基于内部网络的党风廉政、廉洁警示、院内敏感职权使用的防控专网，支持开放对接清廉医院管理系统；（提供截图并加盖公章）

4.1.12内置防统方知识库，且具有独立自主统方学习功能；

4.1.13系统支持虚拟化、虚拟云等网络环境的数据审计功能，准确定位统方行为；

4.1.14系统可针对耗材、药品、检查等涉嫌统方的行为进行审计；

4.1.15可以精确定位可疑对象的物理位置（记录操作人员工号、操作类型、IP地址、客户端工具以及存放路径、操作系统用户名、主机名、MAC地址、SQL语句和操作的时间等关键信息）；

4.1.16发现统方操作后，可以对应相应药品厂家，对该厂商、药代表进行重点监控；

4.1.17能够对数据库操作的结果进行解析，审计内容包含数据库操作结果，并能实现回放功能；（提供截图并加盖公章）

4.1.18用户可以根据需要自定义规则，并能根据设定的条件产生审计报告，能对审计结果进行多条件组合查询，比如按下列条件查询：IP地址、MAC地址、表名、字段名、操作方式（可单独或者多选某种数据库操作）、计算机名、数据库名、程序名（可单独或者多选某个应用程序）等，并就能支持按关键词进行模糊查询，查询结果应支持多种格式(excel、pdf、txt等)导出；（提供截图并加盖公章）

4.1.19支持医院各生产系统中财务数据、病人资料、药品信息、医院资产等核心数据的操作审计监控；（提供截图并加盖公章）

4.1.20产品从审计主体、审计客体、日志格式、规则分析能力、报表、告警、存储等模块完全按照等级保护基本要求和测评要求设计研制；

4.1.21支持对双向数据包的解析、识别及还原，不仅对数据库操作请求进行实时监控，而且还可对数据库系统返回结果进行完整的还原，根据统方行为的特征实时告警；

4.1.22支持审计数据关联准确度，便于审计人员追踪朔源；

4.1.23支持对指定时间内全院抗菌药物的品种、剂型、规格、使用量、使用金额，使用量和使用金额分别排名前N位的品种进行分析，自动生成报表；（提供截图并加盖公章）

4.1.24对于正常合法统方行为，可以在现有防统方系统中做正常统方申请报备处理，在系统呈现统方报表时，给出此操作已完成相应报备手续，属于正常统方范畴；（提供截图并加盖公章）

4.1.25可根据用户自定义规则实时发出手机短信通知和邮件提醒等多种方式的告警信息，并支持配备相应的告警信息发送设备；

4.1.26可以通过移动端收发报警并展示，报表查询，设备状态查看，可以在移动端上进行报备审批等；（提供截图并加盖公章）

4.2.27对于系统捕捉的非法统方行为，需要在医院年度医德医风考评中体现“一票否决”，支持与医德医风系统对接联动；（提供截图并加盖公章）

4.2.28支持分布式部署方式，并支持集中管理功能，可快速查看所有防统方系统的状态、风险状态等；（提供截图并加盖公章）

4.2.29支持医院信息管理系统多层结构，提供全方位的三层的访问审计，可精确定位到人员信息，提升关联准确度和审计人员追踪朔源难度；（提供截图并加盖公章）

4.2.30支持系统管理人员异常操作监控，可按需选择需要告警的操作类别，未开启的操作类别不会发生告警，可以看到具体的告警日志信息，同时支持指定查询某时间段和某类型的告警日志查询；（提供截图并加盖公章）

4.2.31可以监测到 HIS、合理用药，数据中心、SPD等多个系统，如需新增监测系统的数据库，不再额外收取费用；

4.1.32满足院方提出的个性化修改需求。

**4.2硬件技术参数**

|  |  |
| --- | --- |
| **硬件参数** | **硬件需求** |
| **硬件配置** | 2U 机架式设备； 处理器：≥主频3.2GHz，≥4核8线程；内存：≥64G； 磁盘：系统盘250G SSD，存储盘：≥16TB；存储周期不少于1年；接口：千兆电口≥6个；监听接口：万兆光口≥2个；万兆光模块≥2个；支持千兆网络环境及至少4000个客户端并发网络环境监控。 |

**4.3资质要求**

4.3.1产品为专业防统方系统，具备成熟的防统方管理功能，具有“防统方系统”的相关证书，提供加盖公章的证书复印件；

4.3.2提供“防统方系统”的《中国国家信息安全产品认证证书》，提供加盖公章的证书复印件；

4.4.3 制造厂家提供自2020年1月1日至今完成所投产品的同类防统方系统项目业绩合同复印件，须提供合同关键页，关键页包括采购内容（采购内容指可证明与本项目相关的内容）、签订日期 、双方盖章等。

**五、对接口及系统改造的要求**

**质保期和维保期内免费实现以下要求：**

5.1提供全面的接口技术，与第三方系统共享数据和功能，这些接口技术包括中间件技术接口、WEBSEVICE通用接口、数据库级接口、文件文本接口等。

5.2提供与医院第三方系统统一接口的维护与管理，与HIS、电子病历、药品、耗材、LIS、PACS、心电系统、体检系统、集成平台、智慧运营平台、成本管理系统、排班系统、人力资源管理系统、财务管理系统、互联网医院、OA平台、自助服务平台、DRG管理、绩效管理、电子发票、短信平台、财务电子档案等医院所有信息系统进行免费接口对接，实现数据交换。

5.3满足医院电子病历系统功能应用水平分级评价达到6级以上评审、医院信息互联互通标准化成熟度测评达到五级乙等以上水平评审、信息系统安全等级保护三级测评、三甲医院评审、医院智慧服务分级评估标准体系达到4级以上相关的功能要求、医院智慧管理分级评估标准体系达到4级以上相关的功能要求、网络攻防演练中的安全防护要求以及医院其他需要评审的信息化技术改造服务要求；

5.4提供软件免费升级及个性化修改服务，免费实现院方的个性化需求；软件自身错误类问题提供永久性免费修改服务；

5.5免费提供医院新增业务信息系统的对接、免费实现医院上级管理部门要求的系统接口对接要求。

5.6项目不限定用户数、并发数、不限定医疗集团内部及院区使用。

5.7若医院更换已对接的业务系统、乙方须免费提供与新业务系统的对接及联调服务。

# 六、项目实施要求

6.1驻场、实施工期要求：合同签订后，7个工作日内项目实施人员必须进场，系统需在3个月内完成项目实施上线，请分别列出每个系统实施的工作计划及周期。

6.2驻场人员要求：

6.2.1实施工程师：项目驻场实施工程师需有2年以上本厂商同等项目实施经验。项目实施阶段，驻场实施工程师不得少于1名。

6.2.2如需更换实施工程师，厂商需提交书面申请，经院方同意才可更换。

6.2.3竞标文件中需提供软件提供商项目驻场人员清单，清单中标明驻场人员详细信息，如姓名、联系方式、技术职称、社保证明（不少于半年）等。

6.3因厂商与院方存在对需求理解有差异的可能性，要求所有软件功能需求的响应以院方意见为准。

# 七、售后服务及其他要求

7.1自本项目整体最终验收之日起，所有产品要求提供三年的免费质保服务。含软硬件维护和系统软件升级、技术支持服务、系统管理及操作培训，免费提供系统个性化修改需求。请详细说明售后服务的内容。

7.2安装调试要求：免费送货上门、安装调试、提供完善的设备及软件系统使用中文操作手册、图纸、网络详细拓扑图、系统配置、功能配置、设备配置及互联记录；

7.3原厂技术人员免费提供售后服务，含电话支持、现场响应、远程操作、网上客服中心等多种方式服务，应做到7×24小时全天候电话或微信等常用联系方式响应。当出现故障时，接到故障通知后，原厂技术人员应在30分钟内响应，远程技术支持无法解决的，6小时内需到达现场处理修复，并调查分析事故原因，如现场仍不能解决问题，需24小时内免费提供同档次或更高档次的备用设备解决问题。

7.4供应商提供原厂技术人员定期回访服务，定期通过电话或其他方式访问用户，了解产品使用情况及网络安全情况，按院方要求巡检（国家法定节假日前巡检或按院方需求时间巡检），每季度巡检不得少于一次，并形成巡检报告反馈给我院。

7.5免费系统改造，支持国产电脑和服务器以及国产操作系统。

**八、违约责任**

8.1投标方所提供的产品/软件规格、技术标准、材料等质量不合格的，应及时更换，更换不及时的按逾期交货/交付处罚；因质量问题我院不同意接收，投标方应向我院支付违约货款额5%违约金并赔偿我院经济损失。

8.2若投标方提供的产品或软件侵犯了第三方合法权益而引发的任何纠纷或诉讼，均由投标方负责交涉并承担全部责任。

8.3因包装、运输引起的货物损坏，按质量不合格处理。设备安装、调试完成之日起三个月内为设备质保期，在质保期期间若出现设备硬件故障或损坏的情况，我院有权要求投标方更换同等型号和配置的新设备，设备换新、安装、调试产生的所有费用由投标方承担。

8.4 投标方逾期交货/交付的，每天向甲方偿付违约货款额3‰违约金，但违约金累计不得超过违约货款额 5% ，超过30天对方有权解除合同，违约方承担因此给对方造成的经济损失；

8.5售后服务违约：

8.5.1每缺少1次巡检记录，投标方应向甲方支付违约金500元；

8.5.2不能按本技术参数文档第8.3要求中按时提供设备备件的，故障上报24小时不能免费提供同档次或更高档次的备用设备解决问题，每超期一天，按500元/天向甲方支付违约金；

8.5.3 投标方未按本技术要求和响应文件中规定的其他服务承诺提供售后服务的，每次投标方应按合同合计金额的5% 向甲方支付违约金。

8.6合同签订后7个工作日内进场实施，每个模块计划实施周期需在合同内写明。因软件提供商原因逾期不进场实施的，需按每天向院方支付合同款金额3‰作为违约金，超过30天，甲有权解除合同，乙方需承担因此给院方造成的经济损失；不能按照合同约定上线期限完成，需要书面申请说明原因，得到医院书面同意后最多延期一个月，否则（或者延期一个月后）按每超期7天（一周）从总合同金额扣除5%的违约金。扣除比例达到总合同金额的50%及以上的，视为乙方违约，甲方有权单方面解除合同，并要求乙方退回所有医院已支付款项，同时按合同总金额的20%做为违约金支付给甲方。

8.7任何一方违反本技术要求中“保密、廉洁条款”要求的，应承担相应的违约责任并赔偿由此造成的损失，损失累计金额超过合同款项的5%的，损失方同时有权终止合同并收回已付款项。

8.8厂商方未按本技术要求和响应文件中规定的其他服务承诺提供售后服务的，按损失情况，每次应按合同合计金额的0.1‰-0.1%由乙方向甲方支付违约金，损失累计金额超过合同款项的5%的，损失方同时有权终止合同并收回已付款项。

8.9厂商不得在提供的硬件及软件系统中设置包括且不限于如：软硬件加密狗、加密软件、时间锁、授权码等限制硬件及软件系统正常运行的措施，如有特殊需要必须提交纸质文件说明，经过我院签字同意才可设置，否则视为乙方违约，乙方需要支付医院违约金50000元（伍万元），在此基础上医院有权要求乙方退回甲方已支付的所有款项。如对医院造成损失的，甲方有权要求乙方赔偿。

8.10厂商驻场工程师人员变更必须得到医院书面同意，否则视为乙方违约，甲方有权按5000元/人/次从合同总款中扣除。

**九、保密、廉洁协议**

9.1 双方保证对从另一方取得且无法自公开渠道获得的商业秘密(技术信息、经营信息及其他商业秘密)予以保密。未经该商业秘密的提供方同意，一方不得向任何第三方泄露该商业秘密的全部或部分内容，但法律、法规另有规定或双方另有约定的除外。任何一方违反保密义务的，应承担相应的违约责任并赔偿由此造成的损失。

9.2 双方不得以任何方式向第三方泄露本项目的软件技术、设计方案以及功能配置等内容。

9.3不以任何方式向第三方泄露在本协议开发实施过程中获取的经济、技术、数据以及双方其他非公开的信息。

9.4 不从事商业贿赂行为，遵守廉洁协议或相关规定。甲方发现乙方有违反廉洁协议或相关规定采用不正当手段进行不正当竞争行为的，或被有关部门生效文书认定有行贿或者受贿行为的，甲方有权解除该业务合同，由此给甲方造成的损失以及发生的一切费用均由乙方承担，甲方有权对乙方实施商业贿赂不良记录，列入“黑名单”，并三年内取消其业务往来资格。

9.5如有违反《中华人民共和国网络安全法》，则按相关条款规定处置。

9.6保密期限自本合同生效之日起永久有效，如乙方需解除保密协议需向甲方提出书面申请，双方协商同意签字确认后方可解除。

**十、报价**

10.1竞标文件提供技术偏离表、服务偏离表，竞标文件按系统模块报价，报价表价格包含系统软硬件费用、产品安装、调试实施、培训费用、产品升级费用、接口费（包括第三方厂家的接口费）等费用，以及明示所有责任、义务和一切风险。

10.2竞标文件需提供维保期方案及报价。

8.3竞标文件需提供系统详细图文介绍。系统实施验收参照本技术文档及竞标文件提供的图文介绍为依据。

10.4如项目功能二次开发内容涉及我院采购的第三方产品，请在标书内标明哪些功能的实现需要二次开发接口。

# 十一、付款方式

项目双方签订合同，项目上线稳定运行1个月后，用户支付合同款项的30%；合同中所有功能及模块实施完毕，系统上线稳定运行3个月后，启动项目验收，验收合格后甲方支付合同款项的60%，自验收合格之日起，稳定运行1年后，甲方支付合同款项的10%（不计利息）。