一、运维服务目标

需提供基于陕西省互联网医院监管系统的质量保障、技术服务，定期巡检系统以及提供技术支持和应急保障服务，保障互联网医院监管平台业务工作的顺利开展，保证软件系统的平稳、安全运行。

二、运维服务范围

（一）系统基础运维；

（二）系统数据库运维；

（三）系统业务功能与流程优化；

（四）系统与互联网医院接口对接联调；

（五）漏洞的处理修复及其他日常维护；

（六）系统面向使用人员、医疗机构的所有功能模块的维护；

（七）系统使用人员反馈的日常问题处理;

（八）不定期开展系统功能培训，疑问咨询解答等。

三、运维服务具体内容

（一）系统基础运维

全面保障应用系统平稳运行及有效应用：建立系统运维机制。提供全程运维服务，出现故障应能及时告警。必须建立完善的运维机制，包括运维团队、运维方案、运维制度、应急预案等，按月提供运维报告。

（二）系统数据库运维

要求做好对业务系统数据库基础环境和性能维护,保障数据库安全稳定运行，保障业务数据的安全性和保密性，同时配合进行与其他相关业务系统的数据共享。

1.定期对数据库性能优化。结合日常检查、数据库巡检、客户应用需求和客户重大事件，制定数据库系统性能调优工作方案。针对当前数据库运行情况以及收集的性能信息提出系统各项性能参数配置合理调优或硬件扩容建议，在获得客户同意后，对数据库系统各项性能参数配置进行合理调优。

2.开展数据库日常巡检服务，定期检查数据库相关软硬件、数据库配置情况、定期进行数据库本地、异地备份，并对备份数据定期开展还原测试，确定备份数据是否正常。

3.能够开展日常的数据库操作、数据库安全管理、数据备份还原、数据导入导出、数据库漏洞修复等能力，也能进行数据库系统空间合理配置、数据库性能优化、保证数据库和业务系统的稳定运行。

4.省互联网监管平台业务数据库与其他相关业务系统数据共享

按需求与其他业务系统、陕西省全民健康信息平台数据交换枢纽等进行数据共享和对接，满足各业务系统数据需求。

（三）系统与互联网医院接口对接联调

1.按照《陕西省卫生健康委办公室关于互联网医院审批工作的通知》（陕卫办医发〔2020〕35 号），负责卫生健康行政部门同意对接的医疗卫生机构对接陕西省互联网医院监管系统的技术支撑工作，包括但不限于基础数据处理和导入、接口联调测试及指导答疑、网络联通保障、《测试报告》出具等事项；

2.按照中央和省级最新的监管、数据等要求，更新《陕西省互联网医院自建平台数据监管接口规范》；

3.按照省卫生健康委、省卫生健康信息中心的要求，完成各项数据统计任务。完成与医护注册系统（民科系统）的稳定对接，对平台医生、护士等人员进行技术层面校验；

4.提供接口监控预警服务。

（四）系统业务功能与流程优化

按照最新政策文件及省卫生健康委要求，对业务功能和业务流程进行优化，如人员资质监管、医疗价格监管、诊疗全流程监管、护理服务监管等。

（五）系统漏洞的处理修复及其他日常维护。

1.建立闭环漏洞管理流程，保障系统安全与合规性。完成系统在运行中的故障带来的排错工作，解决系统运行故障（除政务云服务商责任外）；

2.如有采购方有要求，需配合完成商用密码评估、信创迁移改造（含操作系统、中间件、数据库改造，以及历史数据迁移和迁移部署）等工作。

（六）系统面向使用人员、医疗机构的所有功能模块的维护

优化业务功能，持续调优性能，提升监管效能与用户体验。

（七）系统使用人员反馈的日常问题处理

系统在使用中的操作问题指导并答疑（包含相关基础数据维护、患者反馈的技术相关问题排查、医生端操作使用相关问题、后台业务数据查询统计等），定期提供系统运营数据分析报告。

（八）不定期开展系统功能培训，疑问咨询解答

四、运维服务要求

1.总体要求

（1）可用性要求

系统：连续工作无阻断，可用率≥99.5%

不出现因系统原因造成用户业务数据丢失事件。

（2）安全性要求

系统安全：避免发生因病毒、木马等外部因素造成业务系统大面积瘫痪；

信息安全：避免发生业务系统数据泄露并造成恶劣影响的事件发生；

（3）及时性要求

事件响应及时率≥95%；

事件解决率≥95%

（4）规范性要求

操作规范：有相应岗位职责说明；有详细的操作指南；有严格的管理制度；有必要的培训；有准确详实清晰完整的工作日志；

服务报告：详细的工作月报，系统评估报告，其他不定期报告（如重大事件的请示报告）和相关工作实施技术方案、工作进展汇报、工作完成情况报告等。

（5）满意度要求

服务投诉事件：用户对运维服务不满意并提出投诉事件每半年不超过3次。

2.服务方式要求

（1）例行检查

每日例行检查：运维工程师通过监控软件加人工巡检的方式对陕西省互联网医院监管平台系统的可用性进行日常检查。

（2）响应支持

通过现场或者远程响应向用户提供7×24小时的热线电话、在线支持、远程诊断和维护、业务培训等运维服务，解答软件系统应用中的各种问题。

3.服务响应要求

（1）人员组织

陕西省互联网医院监管平台系统运维项目组下设一线技术支持、二线技术支持。要求一线技术支持不少于2人，包括项目经理和运维工程师；二线技术支持不少于10人。各运维岗位技术人员职责清晰，分工明确。

（2）服务时间

服务响应时间要求

响应时间指自用户提出故障申告、服务请求之时起，至运维服务提供商开始对故障、服务请求进行处理、用户可查询处理状态之间的时间。针对不同服务优先级，陕西省互联网医院监管系统运维小组将在相应的响应时间内响应，并根据实际情况提供现场服务。具体服务指标要求如下：

优先级1（P1）：10分钟响应，如必要西安市内1小时到达现场；

优先级2（P2）：10分钟响应，如必要西安市内2小时到达现场；

优先级3（P3）：30分钟响应，如必要西安市内3小时到达现场；

优先级4（P4）：以与用户协商的时间为准；一般不超过2个工作日；

服务排障时间要求

优先级1（P1）：2小时内提交解决方案。具体时间与用户协商时间为准。

优先级2（P2）：2小时内提交解决方案。4小时内完全解决事故或明确故障原因；

优先级3（P3）：4小时内提交解决方案。8小时内完全解决事故或明确故障原因；

优先级4（P4）：以与用户协商的时间为准；一般不超过2个工作日；

注：由于运营商问题或用户请求解决的系统终端问题不在上述响应及排障时间内，具体问题需和运营商或用户商定。

4.事件管理要求

（1）处理事件原则

处理事件的原则是尽可能减小对业务的影响；

事件管理流程必须包括管理服务事件影响的步骤，比如评估影响、沟通、提供变通方案等,使事件对用户业务活动的影响降至最小；

在可能的情况下，应该向用户提供继续进行业务活动的手段，即使降低服务级别，比如禁用一项有错误的功能，目的是将事件对用户业务活动的影响降至最小。

5.应急处置要求

陕西省互联网医院监管系统针对安全事件制定应急管理措施，根据符合国家标准GB/Z20986-2007信息安全技术、信息安全事件分类分级指南制定安全事件的等级，将信息安全事件划分为四个级别：特别重大事件、重大事件、较大事件和一般事件。

建立应急组织管理机构、建立应急响应机制、制定应急预案。

6.运维服务安全管理要求

必须确保陕西省互联网医院监管系统的各项信息资产以及客户数据都能得到妥善保护，确保信息的保密性，维持信息的完整性和可用性，防止用户数据的非授权访问。

根据业务要求建立用户对信息的访问规则，并对业务系统和服务的用户访问权的分配建立正式的程序控制；对用户权限和口令进行严格管理。

7.安全环境保障

对业务应用系统进行安全加固有效保障陕西省互联网医院监管系统安全、稳定、不间断的运行。

8.安全管理规范

制定陕西省互联网医院监管系统安全管理规范。

9.保密管理制度

强化信息保密观念，从加强法规制度建设、加强涉密计算机系统保密管理制度建设、加强技术防范能力建设。

10.运维服务制度管理

提供完善的运维管理制度。

五、安全要求

符合截止开标之日还在生效期内的所有跟网络安全、数据安全等有关的法律法规文件的要求；

如果出台新的网络安全方面的法律法规，在项目的运维期，投标单位有义务完成升级，达到法律法规相关要求。

不得使用国家或者行业相关法律法规等政策性文件明令禁止的安全硬件和软件产品、算法、服务等相关内容。

配合建设单位完成本项目有关的安全建设、测评、等级保护（三级）等相关工作。

六、知识产权要求

采购方拥有该运维项目知识产权。项目供应商应根据采购方要求，提供包含不限于项目在进行本招标内容升级开发工作的所有项目升级源代码、项目升级技术文档、数据库相关文档、相关管理员权限、相关超管账户等资料。

项目供应商须保证采购人在中华人民共和国境内使用其提供的服务或其任何一部分时，享有不受限制的无偿使用权，不会产生因第三方提出侵犯其专利权、商标权或其它知识产权而引起的法律或经济纠纷。如供应商不拥有相应的知识产权，则在投标总价中必须包括合法获取该知识产权的一切相关费用，如因此导致采购人损失的，供应商须承担全部赔偿责任。供应商如欲在项目实施过程中采用自有知识成果，须在响应文件中声明，并提供相关知识产权证明文件。