**橡树急诊系统运维服务参数**

## 服务内容

**（一）功能应用维护**

乙方承诺对目前甲方已有的功能模块提供技术维护服务，包括分诊系统、医生站、护士站、质控系统、院前急救系统车载终端、急救平台、卒中中心、高危孕产妇中心、胸痛中心、创伤中心、新生儿中心、服务器及数据库优化。

通过电话、电子邮箱、网络远程、QQ、微信等方式，乙方提供以下服务：

1.提供软件功能的应用咨询，包括功能使用、功能配置、功能设置等，响应时间要求在1小时内完成响应；

2.故障排除方面：协助查找、排除甲方在软件应用过程中出现功能错误及急诊系统各模块模块的故障，保证系统功能正常运行，响应时间要求在1小时内完成响应。

3.报表维护方面：协助甲方进行现有工作报表格式、数据调整、修改，响应时间要求在2小时内完成响应；

4.协助甲方从系统现有数据中修改系统自带报表，新增报表数据超出本系统外，需要从第三方系统（HIS、LIS、PACS等）中获取数据时，乙方需要第三方人员配合完成新增报表的设置，响应时间要求在2小时内完成响应；

5.提供已应用模块范围内的功能需求调整、修改，因甲方需求改变引起的现有系统功能范围内的调整与修改完善（不包括涉及系统整体结构及模块结构改变的需求），并提供详细的文档说明和相关资料，响应时间要求在2小时内完成响应；

6.协助甲方建立日常维护记录，定期与甲方系统管理人员共同检查系统运行情况，并形成系统维护记录制度和系统管理规范，经常性与甲方中心技术人员讨论甲方信息系统运行中存在的问题以及解决方法，响应时间要求在2小时内完成响应。

7.乙方提供已有系统的完善性服务：

（1）现有功能或数据流程的调整：如较复杂的系统参数、本地参数调整；

（2）业务流程的调整：这些业务流程的调整由参数调整完成不了，需要修改源程序以达到甲方功能要求，但该流程调整不会引起系统模型结构的变化；

（3）原有功能的完善：包括操作界面方便、快捷、实用等的调整；

（4）原有报表格式、统计条件、统计口径、数据来源的调整；

1. 已有的报表功能的增强。

8.乙方提供已有系统的适应性服务：

（1）数据字典维护：如一些需要通过后台维护数据库才可实现的字典；

（2）系统定义的参数调整：包括各子系统的运行参数、业务流程参数、运行模式参数等的调整；

（3）由于系统所运行的环境变化，从而软件系统也需变化的调整,该调整不会引起系统模型结构的变化；

（4）由于甲方实际情况的变化，而需要软件做的修改，但此功能的修改不会引起系统模型结构的变化。

二、服务要求

1.服务渠道及服务响应时间

乙方通过电话、电子邮箱、网络远程、QQ、微信、必要时现场维护等方式，提供数据调整服务，因甲方操作不当或其它原因造成患者数据出现部分或全部错误（包括但不限于查找不到患者信息、不能编辑病历信息等），协助甲方系统维护人员查找原因，并对错误数据进行调整，响应时间要求在1小时内完成响应；

2.提供灾难解决办法，系统灾难发生时，乙方承诺立即响应，必要时人员以最快速度到达现场，以减少数据损失，降低灾难对整个系统正常运行的影响。

3.乙方每个季度至少提供一次数据库备份恢复验证服务，保证急诊相关数据存档正确。

4.乙方提供纠错性相关服务，包括但不限于：

（1）程序潜在错误的改正；

（2）由于程序修改或增加功能所引起错误的改正；

（3）数据错误：用户使用系统过程中，由于错误操作而引起的、但通过系统无法挽回的，并且又必须的数据，由当事人提出申请，并经过相关人员批准后，将错误数据纠正。

5.培训要求

（1）根据甲方需求，乙方对各岗位计算机管理系统维护管理人员进行岗前的技术培训。了解软件系统内包含的管理思想、管理流程。

（2）乙方提供系统维护培训服务，包括甲方岗位调动、系统维护人员上岗前的培训。

6. 现场巡检服务

乙方提供一年三次，每次不少于三个工作日的巡检服务，到甲方现场检查系统模块运行情况，与甲方维护人员沟通，提供常见问题的解决办法，巡检结束后给甲方提供巡检报告；

7.乙方提供维护热线，并为甲方建立维护档案，给予及时的系统支持；

8.乙方帮助甲方建立日常维护记录制度和系统管理规范；

9.乙方解答甲方关于系统和数据库的疑难问题；并提供数据库操作的解决方案；

10.乙方应保证系统整体运行稳定，并且在本产品范畴内，根据甲方实际需求进行各模块功能版本升级；

11.乙方按照国家传染病监测平台要求，对急诊所涉及内容进行数据接口对接，时间为40个工作日内；

12.乙方提供已有功能模块的评级/迎检服务支持（包括但不限于实证截图，数据质量等国家评级要求内容），甲方在进行电子病历、智慧医院等评级时，可提前预约乙方进行远程或到甲方现场进行服务支持。为评级后相关整改或问题查找提供支持。

13.安全要求

服务期内配合甲方定期开展网络安全自查，自查内容至少包括系统日常运行情况、系统漏洞等；配合甲方定期进行安全审计，审计内容至少包括系统账号、权限、操作行为和安全技术措施有效性等，及时发现和处理信息系统运行过程中的安全隐患，减少或避免网络安全事件的发生。