序号	分类	具体需求
1.	整体性需求	合规性及稳定性 系统必须遵循 NMPA、FDA、ICH-GCP 等国内外相关法规和标准的要求，并且具有一套完整的、NMPA 和 FDA 以及国内外申办方认可的验证体系，可以提供符合相关法规或指南的证明材料。 系统成熟、实用、能够长期保持技术先进性，且在国内、外有大量的用户基础，和 I 期临床试验成功应用案例。可提供国内三甲医院 I 期临床试验用户信息，或国外医院用户信息。
2.		功能全面 满足 I 期临床试验全流程自动化，功能应贯穿于早期临床研究各个环节，从设计 CRF、志愿者招募、受试者筛选、采集试验数据、CRF 变更、处理 PK/PD 样本，到最后的数据清理、数据库锁定以及试验资料存档。 提供以上所有功能的详细证明材料，可以是详细的文字描述，也可以是产品官方宣传文件。 根据实际工作需要，负责与院内 LIS、PACS 等软件对接（含对接所发生的一切费用）。 整体信息化功能上线前、中、后培训工作，要求现场对全部工作人员培训。 提供 7*24 小时售后服务，满足后期系统维护、更新等。
3.		支持中文、英文等多语言，便于进行国外项目申报及国外申办方进行远程核查及稽查，满足国内、国际双申报要求。提供软件英文等语言操作界面的截图证明。 系统支持中文、英文等多种语言，满足国际临床试验对于语言的要求。系统同时符合国际 CDISC 标准，能够满足国际双申报的格式要求。 提供国内（含港澳台地区）、国外使用或申报的案例证明； 提供使用投标产品进行的临床试验通过核查证明文件。
4.		支持多点部署 系统应是 B/S 架构，基于浏览器登录，在任何地点，只要有网络，均可以登录浏览器进入系统， 方便异地多中心的使用和管理。
5.		兼具 eSource & EDC 的功能 应同时具备 eSource 和 EDC 的功能，试验过程所有的操作记录均可自动记录到系统的电子 CRF 里，系统中的数据即为源数据，在本系统内即可进行质疑、答疑、数据审核、锁库和解锁，并保留下记录，源数据采集和统计一次完成，无需二次转录到其他 EDC 系统。
6.		灵活设计操作流程 系统应能根据临床方案，研究机构的操作习惯灵活设计操作流程，并在操作过程中根据设计进行控制。
7.		稽查轨迹 系统应能在数据采集的同时，记录下操作者信息和操作时间以及操作结果，并将这些信息传输到服务器上永久保存，任何修改将会留下稽查轨迹。同时，还可打印稽查轨迹报告，可清晰地重现数据创建、修改、删除有关

		的事件过程以及用户登陆、登出的痕迹。 提供该功能的详细介绍和对应功能的软件截图。
8.		支持国际通用医学编码 系统应能支持国际通用医学编码，支持内置国际通用英文医学编码字典。 提供该功能的详细介绍和对应功能的软件截图。
9.		试验过程中的方案变更 系统应能支持研究期间因各种原因需要修改试验方案的操作。 提供该功能的详细介绍和对应功能的软件截图。
10.		设盲 支持开放研究，单盲、双盲、三盲等多种盲法设计。
11.		完善的系统验证 应进行充分的系统验证，具有一套完整的、 NMPA 和 FDA 以及国内外申办方认可的中、英文验证体系。系统验证应符合《临床试验的电子数据采集技术指导原则》、《临床试验数据管理工作技术指南》以及 NMPA 和 FDA 有关计算机化系统验证的要求。
12.		远程监查 支持远程监查、实时质控，研究者和监查员可在任意时间和地点远程访问系统，了解试验进行情况和数据质量，及时处理。
13.	具体功能参数需求	方案设计 1、支持研究病例/CRF 一体化设计，CRF 数据取自研究病例； 2、 根据试验需要，对任意事件设定时间窗，操作人员需遵循时间窗，如果超窗，或规定时间点没有操做会有提示； 3、 基于 I 期临床试验的流程和时间点来设计 eCRF； 4、 满足适应性设计临床试验的需求，可以提供灵活的 CRF 变更； 5、 数据库搭建操作简单； 6、 数据库模板化设计； 7、 系统支持对 eCRF 设计进行简单的逻辑核查； 8、 支持根据不同的角色进行权限的分配； 9、支持试验进行中因方案变更而需要临时修改 CRF 的操作。 10、支持内置国际通用的 MedDRA 和 WHO Drug 英文医学编码字典。 11、能够实现 eCRF 的版本控制，且能够实现变更前后的对比； 12、支持条码设计和分配，用于受试者和事件或仪器的确认。 提供该功能的详细介绍和每个功能点对应的软件截图。
14.		受试者招募 1、 包含志愿者招募管理功能，可自定义招募模板，采集志愿者信息； 2、 支持志愿者在招募网站自己提交注册信息，也支持招募公司和研究机构填写注册信息（支持院内、外提交注册信息）； 3、 支持受试者管理，可以自定义筛选标准，给志愿者添加标签，如高血压、糖尿病、筛选、脱落（包括但不限于），可以通过这些标签来进行快速检索；

		4、 受试者所有的信息包含在试验期的 AE 记录等也可同时记录在受试者库里，方便后续检索； 5、 可以实现对受试者信息的批量更新； 6、 系统支持向志愿者发送短信等通知或邀请； 7、 支持导出志愿者信息资料报告。 提供该功能的详细介绍和每个功能点对应的软件截图。
15.		数据采集 1、 支持按照设定的操作流程执行试验； 2、 能够集成临床常用的医疗设备，如身高体重秤、电子血压仪、心电图机等捕获数据，数据实时记录； 3、 能够自动生成采血管和冻存管条码； 4、 支持通过扫码等多种方式进行采血计时，同时可以使用条码打印机、扫码枪打印条码和识别受试者、样本及仪器的身份； 5、 支持自定义各种检验项目的正常值范围； 6、 实时稽查轨迹，数据的创建、修改、删除等都会在系统永久保存； 7、 数据留痕，所有操作人员在数据采集的同时，系统将记录下操作者信息和操作时间以及操作结果； 8、 具备准确、完整的审计追踪功能； 9、支持电子记录和电子签名，符合国内、外 FDA 21 CFR Part 11 相关法规； 10、通过中心实验室数据 HL7 传输协议，可实现实验室检测结果的自动导入。 11、系统应能与 LIS 系统进行对接，使得实验室检测结果及正常值范围等直接传输到系统中。 12、同时系统还应支持自定义各种检验项目的正常值范围，并能在无需编程的情况下实现 Edit Check。 提供该功能的详细介绍和每个功能点对应的软件截图。
16.		样本处理 1、 根据研究方案设计样本处理的流程，并详细设定时间、温度等参数； 2、 系统能通过扫码来辅助确认采血管和冻存管的对应关系，错管，系统应有提示。 3、 支持在系统内建立虚拟的实验室设备，入冰箱、离心机，支持样本的快速检索和报告； 4、 支持对样品从采集到接收、离心、分装整个过程进行追踪，并追溯样本存储的物理环境（接收、离心、分离、存储）。 5、 可通过扫码快速记录样本的操作，进行实时记录，并能在线为实验室样品处理人员提供样品处理说明； 6、 支持对样品进行批处理，方便样品的大批量处理、存储和运输。 7、 支持系统条码和外部条形码。

		提供该功能的详细介绍和每个功能点对应的软件截图。
17.		数据管理 1、支持逻辑核查，在用户输入数据时触发逻辑核查，通过实时采集让研究者可以在第一时间对数据进行核查； 2、支持质疑发起和处理，将质疑发给指定的角色和用户，还可以通过短信等及时通知相关人员； 3、对采集的数据进行审核，可支持≥3 级的数据审核； 4、支持远程监查、实时质控，监查员可在任意时间和地点远程访问系统，了解试验的进行情况和数据质量，及时应对处理； 5、支持数据的软锁定和硬锁定； 提供该功能的详细介绍和每个功能点对应的软件截图。
18.		数据导入与输出 1、系统应能从外部数据源（比如实验室、电子 ECG 系统等）导入数据； 2、也能将产生的数据进行导出和一键存档； 3、系统应包含临床研究常用的报表（如注释 CRF、空白 CRF、质疑报告、稽查轨迹等）及自定义报表； 4、导出符合统计要求的数据集，包括 SAS 数据集； 5、支持包括但不限于 SDTM 标准格式导出，符合 NMPA、FDA 的递交标准； 6、导出相关法规要求存档的电子记录资料； 7、导出各类法规要求的报告，比如稽查轨迹，质疑报表等； 8、在数据传输和数据导出过程中确保数据加密； 9、导出与导出文件支持主流通用电子表格文件，如 Excel，Wps 表格等。 提供该功能的详细介绍和每个功能点对应的软件截图。
19.		数据存档 1、预设不少于 30 份系统报告，包含临床研究常用的报表，如空白 CRF、质疑报告、注释 CRF、稽查轨迹等。 2、支持一键存档、定时存档，包括完成的 CRF、稽查轨迹以及所有上传的附件等。 3、 存档格式支持 PDF、图片等格式； 提供该功能的详细介绍和每个功能点对应的软件截图。
20.	硬件要求	服务器： 数量：2 台 1、总体要求：2U 标准机架服务器。 2、处理器：配置≥2 颗国产 X86 CPU，单颗性能≥2.8GHz/16 核。 3、内存：配置≥128GB 3200MHz DDR4 内存，配置≥32 个内存插槽。 4、存储：配置≥1 块独立 RAID 卡，2G 缓存，带断电保护模块，支持 RAID 0、1、5、6；配置≥2 块 900GB SSD 硬盘。 可扩展≥30 个硬盘槽位。 5、网卡：配置≥2 个万兆光口（满配光模块），≥4 个千兆电口。

		6、电源风扇：冗余风扇，配置≥2 块冗余电源模块。 7、管理和维护：配置服务器批量管理系统，支持批量自定义安装操作系统，满足在批量安装 OS 过程中对分区、软件包等安装设置进行个性化定制的需求。 8、配置服务器管理软件，支持通过 U 盘下载服务器日程日志系统日志，实现应急诊断。 9、服务：提供生产厂商三年 7*24 小时售后服务，并提供生产厂商三年售后服务承诺函。
21.		平板电脑： 数量：20 台 1、 CPU 核心数：≥8 核 2、 处理器速度：≥2.9GHz 3、 运行内存：≥16GB 4、 存储容量：≥1TB 5、 系统：Windows 10 或以上 6、 网络连接：WiFi 或 WLAN 7、 含键盘 8、 屏幕尺寸：≥12 英寸
22.		条码打印机： 数量：6 台 1、分辨率：203 dpi（8 点/mm） 2、打印方式： 热敏或热转印 3、打印速度： 5 英寸（≥150 mm/秒 ） 4、打印宽度： ≥100mm 5、打印长度： ≥39 英寸（991 mm） 6、字体/字符集： 繁体，简体中文字体集 7、介质类型： 卷筒或折叠纸，标签纸，tag 材料，收据纸和腕带
23.		条码扫描枪： 数量：8 台（桌面台式）、12 台（便携式） 1、扫描速度：≥每秒 72 条扫描线 2、扫描角度：水平 50° 3、系统接口：RS232 串口，键盘口 4、扫描精度：不低于 3mil 5、解码类型：一维 6、传输方式：有线传输 7、光源：激光

		8、扫描介质:纸质 9、抗震能力：0-1M
24.		脚踏开关： 数量：6 台 1、材质：钢或铝合金 2、防护等级：≥IP54 3、可模拟键盘功能，USB 接口即插即用，无需安装驱动
25.		腕带： 数量：30 卷 1、 成人热敏腕带 2、 尺寸 L269mm*W25mm
26.		碳带： 数量：30 卷 1、 树脂碳带 2、 尺寸 60mm*80mm
27.		标签纸： 数量：15000 枚 1、常温标签纸： 尺寸 50mm*30mm，3000 枚 2、低温标签纸： 尺寸 28mm*24mm，12000 枚
28.	网络安全保障要求	服务器杀毒系统: 数量：1 套 1、产品采用 B/S 架构，支持通过 HTTPS 方式登录管理控制台，管理控制台访问需进行加密访问。 2、支持主流商用数据库，至少满足 Microsoft SQL Server、Oracle Database、 PostgreSQL、MySQL。 3、支持主流 Windows 操作系统，包括 Windows Server 2008 （32/64Bit）、Windows Server 2008 R2 64、Windows 8 （32/64Bit）、Windows 8.1 （32/64Bit）、Windows 10 （32/64Bit） 、Windows Server 2012（64Bit）、Windows Server 2012 R2（64Bit）、Windows Server 2016 （64Bit）、Windows Server 2019 （64Bit）。 4、支持主流 Linux 操作系统，包括 Red Hat Enterprise Linux 、CentOS Linux 、Oracle Linux 、SUSE Linux 、Ubuntu Linux 、Debian Linux 、Cloud Linux 、Amazon Linux 、中标麒麟、银河麒麟、普华 Linux、华为欧拉、中兴 Linux 等。 5、产品功能包括不限于防恶意程序、 Web 信誉、完整性监控、防火墙、

		入侵防御（DPI）功能。（提供截图并加盖原厂商公章） 6、支持对不同类型的恶意软件配置不同处理动作。 7、支持配置实时扫描生效时间段；支持扫描嵌入式 Microsoft Office 对象配置；支持扫描例外配置进程镜像文件列表；支持可疑文件外发沙盒模块分析；支持扫描缓存配置；支持检查可疑活动和未授权的更改（包括勒索软件），并提供备份、恢复勒索软件加密的文件。 8、产品具备恶意行为监控功能，支持检测可疑活动和未经授权的更改。 9、产品支持通过预测性机器学习为未知威胁和零日攻击提供增强的恶意软件防护。（提供截图并加盖原厂商公章） 10、产品可以实现与外部沙箱实现集成，同步沙箱的检测结果，检测未知威胁，并处理。 11、支持配置监控的 Web 页面端口，配置阻止 Web 页面是否显示本地通知，配置阻止 Web 页面是否触发警报。 12、产品支持推荐扫描，根据不同计算机的扫描结果自动下发对应的入侵防御规则。 13、入侵防御功能支持自定义新增入侵防御规则。 14、支持生成报表，可指定任意虚拟机/终端、计算机组、策略、时间段和标记进行报表生成，包括数量排名、图像展示；支持定义报表保密级别；支持生成报表加密。 15、产品具有虚拟化安全防护（增强级）销售许可证。（在投标文件中附加盖厂商公章的证书扫描件）。 16、提供厂商针对此项目的三年售后服务承诺函。 服务器安全防护授权数≥2 个，病毒特征库升级服务≥3 年，深度包检测特征库升级服务≥3 年。
29.		安全风险评估服务： 数量：1 项 1、针对本次招标系统提供安全风险评估服务，出具安全风险评估报告，报告需加盖服务商公章。 2、安全风险评估包含初测和复测两个环节，复测在确认所有已发现的漏洞修复完成后结束。 3、恶意代码：查看系统相关业务系统和网站，是否存在恶意上传的脚本，是否存在可疑目录，是否 存在可疑文件，检索是否存在常见 WEBSHELL、网页木马等常见恶意代码。 4、备份文件：查看系统相关业务系统和网站，是未删除的备份文件和备份的网站目录。 5、WEB 安全漏洞 Web 远程渗透测试专项由服务厂商从远程采用技术检查的方式对系统相关业务系统进行渗透测试，安全结果以厂商测试结果为准，系统相关人员可以通过以下方式进行自查， 检测项目包括但不限于以下所列内容。 SQL 注入：查看系统相关业务网站代码安全，是否存在输入和查询过滤不严，造成 SQL 注入漏洞，利用该漏洞查看、插入、删除数据库的数据，甚至可以执行主机的系统命令。 备份页面泄漏：查看系统相关业务网站，是否未删除的备份页面，此类页

		面可能造成源码 下载和文件路径泄露。 版本管理文件泄漏：查看系统相关业务网站，是否可以对版本管理文件进行删除和禁止访问。 管理后台泄漏：查看系统相关业务网站，管理目录是否暴露在公网中。 错误详情泄漏：查看系统相关业务网站，管理目录是否暴露在公网中。 跨站脚本（XSS）：查看系统相关业务网站，查看是否存在 XSS 漏洞,此漏洞可用于触发 cookie 盗窃、帐户劫持、拒绝服务攻击等各种攻击。 上传攻击：查看系统相关业务网站，查看是否存在任意文件上传，或者对上传文件没 有进行格式校验。 远程命令执行：查看系统相关业务网站，查看是否存在远程命令执行漏洞，该漏洞可以执 行系统命令。 认证绕过：查看系统相关业务网站，查看是否存在认证绕过漏洞。 最新 web 漏洞测试专项：最新 web 漏洞测试专项由服务厂商从现场采用技术检查与访谈的方式对相关业务系统进行专项测试，安全结果以厂商测试结果为准，系统相关人员可以通过以下方式进行自查，检测项目包括但不限于以下所列内容。 6、常见框架安全漏洞 Struts2 远程代码执行漏洞：检查系统相关业务系统中是否存在 Struts2 远程代码执行漏洞。 Thinkphp 远程代码执行漏洞：检查系统相关业务系统中是否存在 Thinkphp 远程代码执行漏洞。 在线编辑器漏洞 ewebeditor 在线：检查系统相关业务系统中是否存在有漏洞的 ewebeditor 编辑器。 7、常见第三方组件漏洞 TRS 拓尔思发布系统安全：检查系统相关业务系统中是否存在有漏洞的 TRS 内容发布系统。 DeDecms 软件安全：检查系统相关业务系统中是否存在有漏洞的 dedecms 开源系统。 Discuz!软件安全：检查系统相关业务系统中是否存在有漏洞的 Discuz!论坛系统。 8、用户登录机制安全性 静态密码登录机制：查看用户在静态密码登录机制、动态密码登录机制、用户登录监控机制以及 密码找回机制中是否存在口令破解风险、恶意密码重置风险、动态短信验证码破 解风险以及口令明文传输风险等。
30.	其他要求	1、自验收合格之日起软硬件 3 年质保期。每年由工程师提供至少 4 次的免费上门维护保养工作。 ※2、质保期内服务：根据甲方管理要求，为甲方指定的第三方的业务开发提供必要的技术支持，免费提供相应的数据接口和程序接口服务，不再额外收取接口费用。 3、中标方应对系统使用人员进行操作培训，直至使用人员熟练掌握为止，提供详细培训记录。 4、维修保障：提供中文说明书、操作手册、质保期内软件免费升级。 ※5、服务期内，派驻软件系统原厂工程师至少 1 人，按照甲方管理要求

		工作，严格遵守甲方规章制度及科室管理制度，负责提供技术咨询、故障排除、现场支持等具体工作，定期巡检及调优系统。 6、全年内7*24小时响应,如驻场工程师电话或远程等方式不能解决问题，需2个小时内到达现场解决。