立项需求技术参数书

1. 项目名称：中山大学附属第一医院骨肿瘤科科研数据库项目

二、项目概况与设备数量：

骨肿瘤科科研数据库的建设，将极大的方便大量临床数据资料的高效录入、存储和调用，整体需求包括：医院现有的HIS、LIS、PACS等数据，可与平台或数据湖无缝对接，或通过数据文件批量导入方式，整合数据，整合的数据可通过病人唯一ID号进行检索；

实现图像、文字集中统一存储：将临床的图像及病人文字报告资料集中存储；

实现图像、文字科内共享：获得授权的院内内网电脑均可浏览图像、文字资料，方便科室统计、分析和管理，特别是自动查找复查病历、历史病历对照；

特殊病历标记：可将特殊病历进行分类归档，方便用于教学、学术等；

实现科研数据管理：建立科研数据库，实现科研项目管理、科研成果管理及科研随访等全方位科研管理；对于需要长期追踪的数据项，能够根据时间轴进行区别统计，可视化展示；

对于具有潜在关联的数据项，可以通过大数据统计分析，建立关联。

建立具体模型算法，通过临床实际病例，反复校验调整，直至建立精准模型，形成专利、著作权和科研文章等知识产权，并服务于临床。

1. 技术参数及配置要求：

（一）总体要求

1、系统架构：系统应尽可能使用B/S架构建设，方便系统维护升级；

2、多终端：需支持移动端、PC端（兼容主流浏览器软件，如360、谷歌、火狐、IE等）使用；

3、系统界面：系统界面简洁友好功能设计合理、全面，方便科室人员操作；

4、权限设置：满足各建设科室业务功能场景需求，支持对用户权限、角色权限、数据权限进行分配与管理；

5、专病数据库系统需支持应用功能的横向拓展，如对接第三方应用、多中心覆盖或基于各临床科室需求进行的定制化功能研发；

6、支持丰富的数据对接方式：支持与医院现有HIS、LIS、PACS、EMR、护理系统、病理系统、数据湖、科研数据平台等进行对接，获取相应专病患者数据信息，并支持与后续新建业务系统进行数据对接；数据对接支持多种形式，包括数据推送、ETL、API接口、文件等；

7、与医院信息平台互联互通，满足医院无纸化、统一登录、主数据、系统传输日志监控等的管理要求；

8、数据安全：采取措施保障数据的完整性与保密性；网络前端入口设置防火墙，阻挡恶意攻击；系统需满足医院医疗数据安全保护要求并通过安全测评或等保认证，详见“（3）医院信息安全等级保护三级要求；”

9、数据备份与恢复：支持进行实时、本地、远程数据备份和离线备份，保证数据安全；具备完善的系统灾备方案，能快速恢复数据，保证业务持续；具有容错、容灾功能。

（二）功能需求

| **编号** | **主模块** | **子模块** | **功能列表** | **功能详情** | **模块说明** |
| --- | --- | --- | --- | --- | --- |
| 1 | 基础模块 | 用户管理 | ★新建用户 | 填写用户昵称，填写归属部门，设置用户角色，账号状态，用户名称，用户密码，手机号码，用户性别，以及账号备注。 | 平台账号状态管理，平台账号信息管理，平台账号的使用管理（重置密码。修改各项信息） |
| ★搜索用户名称 | 搜索用户名称 | 　 |
| ★手机号码 | 搜索用户手机号码 |
| 角色管理 | 新增角色 | 新增角色名称，权限字符，角色顺序，角色状态，设置菜单权限，以及角色备注 | 设置各种角色的权限职责，设置角色的数据范围，修改权限范围 |
| 角色列表 | 设置角色状态，修改角色状态，删除状态。 | 　 |
| 机构管理 | 新增机构 | 设置新增机构的上级部门，部门名称，显示排序，负责人信息，联系电话，邮箱以及部门状态。 | 平台入驻医院的状态管理 |
| 发布公告 | 发布平台级别公告 | 让每个用户都能收到公告通知 | 发布平台级别公告，全平台账号都可收取信息 |
| 医院管理 | 新增医院 | 选择医院类型，治疗医院或者随访医院，设置排序，医院名称 | 平台参与医院的属性管理和使用状态管理 |
| 2 | 首页 | 工作量统计 | 工作量统计图表 | 显示医院的工作量排名，医院名称，病历上传数量百分比统计图 | 查看所有医院的工作量排名，以及详细的院内各个账号的工作量以及质控信息 |
| 统计图表 | 工作量统计图表详情 | 显示病例总量，连入医院数量，本月上传病历总数，医院列表，病历录入情况，总览病历性别，年龄，手术方式，病理诊断，癌变组织等统计图。 | 查看目前平台连入医院数量，本月平台整体病历上传输，各家医院的录入情况，录入排名列表 |
| 统计总表 | 设置关键值筛选 | ▲按照关键值筛选出关键值形成表格 | 查看平台全部病历的部分关键信息：性别、年龄、手术部位、最终追加治疗等信息 |
| 3 | 数据采集 | 数据源分析 | 院内业务数据对接 | 支持获取院内业务系统中满足入组条件的患者所有在院诊治信息：包括住院或门诊信息（个人信息、诊治科室、诊治时间、手术记录、治疗方式、治疗药物等）、全院所有检验及检查信息等；支持通过基于业务系统原始数据和数据湖工具自行构建API接口的方式进行供给，和手工录入实现供给，如采用手工录入的方式，如采用手工录入的方式，成交服务商需提供足够的人力进行录入支持。 |  |
|  | 生物样本库对接 | 支持获取医院现有生物标本库，获取入组患者的生物样本数据 |  |
|  | 院外数据对接 | ▲支持在基于固定结构化表单的格式下开展患者院外数据录入，包含诊断报告，手术记录，门诊、住院病历等院外患者诊疗数据，并支持多种格式的图片及视频上传；支持获取以检验、检查报告为主的患者院外图片数据，通过图像识别技术，准确提取相应结果报告中的数据；如采用手工录入的方式，成交服务商需提供足够的人力进行录入支持。 |  |
|  | 专病库数据对接 | ▲支持对科室原有专病库数据进行获取，如采用手工录入的方式，成交服务商需提供足够的人力进行录入支持。 |  |
|  | 数据采集规则 | 住院患者采集规则 | 全院所有科室收治的骨肿瘤科患者，由出院诊断确定 |  |
|  | 门诊患者采集规则 | 全院所有科室门诊诊断包含骨肿瘤患者，由诊断信息所确定 |  |
|  | 采集数据范围 | 科室要求的历史数据范围及未来增量数据 |  |
|  | ETL采集 | ETL采集引擎 | 1、支持具备从多种不同的数据源（ORACLE、SQLSERVER、MySQL、VIEW、消息、HL7、WS）中进行指定规则的数据提取作业；2、支持具备数据转换功能，在数据提取的过程中将不同数据源、不同数据类型的数据进行转换；3、支持具备数据装载功能，平台默认以1000条缓存数据为限，每达到限制数量后执行一次数据装载，并可根据单条数据量大小来修改单次装载量，支持动态配置；4、支持全量数据/增量数据采集同步；5、指定时间间隔或指定时间点进行自动采集；6、支持对数据采集过程实施监控预警；7、如采集任务异常中断，支持一定时效内的自动重启恢复，如多次重启失败，则支持记录同步状态，提交给数据监控预警并生成后端日志文件保存；8、病例数据被采集进入专病库服务器后，支持根据科室提供的入组条件自动核查病例是否符合入组规则，并将符合的病例与不符合的病例分组存储（如入组病例组a、备用病例组b）；9、病例入组的手工修正：支持科室对病例组归属进行修正，将入组病例组中的没有科研价值的病例排除，或将备用病例组中的病例手工标记入组；10、入组原因标签：对于入组病例，支持显示病例的入组原因（因符合哪一条入组条件而入组，或因哪个用户的操作而入组）；11、批量排除：支持系统管理员基于入组条件或检索条件从入组病例组中批量排除符合某特定条件的病例。 |  |
| 4 | 基础信息管理 | 病例总表 | 病例列表 | ★显示患者序号，患者姓名，年龄，性别，治疗医院，手术日期，病理学结果等信息 |  |
| 患者检索 | 数据检索 | 1、专病普适检索业务域需包含人口学信息、就诊信息、诊断信息、一般检验、微生物检验、检查报告、医嘱记录、门急诊病历、住院病历、入院记录、出院记录、病案手术等在内；▲2、支持对检索出来的患者数据结果进行二次字段检索，并可针对某些后结构化数据元实现进一步细分，如实现到具体字段数值范围或值域范围的筛选；3、用户可将感兴趣或最近在做课题的检索条件进行收藏，方便下次直接调用检索；4、支持保留历史检索条件，实现快捷检索条件调用；5、支持一键清空添加的检索条件，恢复检索功能初始视图；6、支持对检索出来的结果进行概览可视化展示，如患者总数、性别/年龄占比、诊断词云图等；7、支持将检索出来的患者一键全量/批量勾选添加至科研队列/随访队列，或同时添加至两个队列，开展后续前瞻性跟回顾性研究； |  |
| 导出 | 数据集导出 | 根据数据集需要的字段检索出数据之后导出Excel表 | 可以根据数据集检索出数据之后批量导出Excel表格数据 |
| 全量导出 | 勾选数据全量导出Excel | 　 |
| 添加病例 | 添加病历内容 | 术前信息 | 包括人口学信息、病史信息、影像学信息、实验室检查信息、用药信息、手术信息等，要求使用病例的表格化录入页面，以用来后续的数据分析及结构化模型训练。 |
| 术中信息 |
| 术后信息 |
| 出院信息 |
| 随访信息 |
| 5 | 数据质控 | 数据质控功能 | 系统自动质控 | ▲系统内部针对数据类型、数据值域等规则进行自动质控 | 科室内审核员来确认目前病例总表中的数据是否达到可用标准，可以通过病例-驳回病例-存疑病例等。 |
| 数据人工审核 | 病例提供人工审核模块，设置通过及驳回机制 |
| 6 | 文献库 | 文献列表 | 查看与管理文献 | 　 | 查看和管理目前的文献列表 |
| 上传文献 | 上传文献包 | 以文件夹的形式上传文献内容 | 上传pdf格式的文献材料 |
| 7 | 科研中心 | 数据集管理 | 新建数据集 | 选择目前数据库中的数据字段，保存数据集方案。 | 查看目前的正在使用的数据集，可以开放或者关闭个人数据集检索方案。新建个人数据集，能够自定义全局字段，搜索规则等，保存方案之后可以在病例总表中使用数据集。 |
| 管理数据集 | 查看数据集列表，修改或删除数据集 | 　 |
| 病例数据更新提醒 | 更新数据 | 后续随访数据有更新时提醒医生有新数据 | 数据更新机制 |
| 科研课题 | 创建课题 | ▲创建课题，设置课题类型，课题名称，数据收集表，牵头单位，牵头单位负责人，牵头单位负责人电话牵头单位负责人邮箱，参与单位，参与单位负责人参与单位负责人电话，参与单位1负责人邮箱，课题开始时间，课题结束时间，课题目标样本量。 | 查看目前启动中的科研课题项目列表，可查看课题详情，加入课题，以及退出目前正在参与的课题。填写相关课题信息以及邀请参与的科研单位，设置课题时间，结题时间，样本数量等。 |
| 我的课题 | 查看我加入的科研课题 | 查看和管理目前已在队列中的科研病例 |
| 科研病历 | 病历详情 | 查看根据数据集筛选出来的科研病历。 | 使用数据集检索所有数据之后，自定义目前显示的表单模式，支持更改各项表名，表单位置的设置，如未设置表单，系统可提供基础表单选择。 |
| 模板编辑 | 根据自己实际的科研流程状态，编辑表单的各项填写框的顺序以及表单布局，可提供多种表单布局使用。 | 　 |
| 患者标签 | 1、支持对患者进行打标签操作，用来标识患者状态；2、拥有同一标签的患者将默认进行关联，在队列级的检索、亚队列纳入和数据导出时，可以直接通过患者标签进行操作。3、支持纳入队列研究：具备相应权限的用户可将项目中的患者纳入到科研/随访队列中开展相应研究；4、支持对项目患者列表中患者数据进行二次检索，二次检索的结果队列亦可直接被生成或纳入到科研/随访队列中开展相应研究 |  |
| 导出 | 导出病例信息 | 导出Excel文件 | ▲以Excel的方式，导出目前科研队列里的全部数据。 |
| 8 | 随访管理 | 随访列表 | 随访任务 | 一定周期内等待随访的患者， | ▲随访队列状态支持通过短信或微信通知；并能通过短信或微信的形式发送随访问卷。 |
| 失访列表 | 一定周期内失访的患者 |
| 随访规则 | 自定义时间区间来筛选随访患者。 |
| 随访计划 | 根据数据集检索出来的患者的随访情况 |
| 随访导出 | 导出完成、进行中、失访的人员名单 |

（三）医院信息安全等级保护三级要求

1、账户安全管理要求

1.1 面向互联网的应用，用户注册及登录均需要验证码。验证码须在后端进行校验。

1.2 系统支持用户凭验证码找回密码功能，验证码位数6位或以上；

1.3 强制用户首次登陆修改密码；

1.4 输入密码时，默认在屏幕上不显示明文密码，可提供密码明文显示按钮；

1.5 首次输入密码可不用验证码，输入密码错误时强制弹出验证码;

1.6 通过手机短信接受验证码时，须要求事先校验手机号正确再发送短信；

1.7 限制单位时长内短信验证码发送次数，60秒1次，发送次数在服务端校验；

1.8 密码至少10位（含）以上，强制要求由数字、小写字母、大写字母和特殊符号4类中至少3类组成，且支持使用键盘上的任意特殊字符构成密码；

1.9 支持定期强制修改密码功能，定期改密的周期应可配置。（如：可配置密码改密周期为一个月或一年不等），支持到期前一个星期提醒用户更改密码的功能，并禁止使用原有密码；

1.10 支持密码连续输错若干次将锁定账户的功能，次数可配置（如：5次），设置定长时段后自动解锁账户（如10-30分钟）；

1.11 账户密码必须以加密的形式存储或传输，采用md5+salt、sha-256摘要算法，或国密算法，符合等保要求；

1.12 密钥文件不得以明文方式存储在应用系统；

1.13 禁止将密码（密钥）从服务器发往前端进行验证；

1.14 应用系统中数据库配置文件中的连接字符串须加密（如 实例名、服务器IP、账户名、密码等）；

1.15 支持会话空闲超时中断的功能，时长参数可配置（如， 15分钟）；

1.16 建议账户名由字母或字母加数字组合，建议6位以上。

1.17 系统支持设置账户有效期，到期自动禁用。

1.18 系统支持账户的停用、启用、注销功能，可限制用户对系统的访问时段；

1.19 系统支持账号名模糊匹配、创建时间、登录次数、账号状态、末次登录时间、末次维护时间等条件查询功能，支持查询结果账号列表批量停用账户功能，并预留解冻功能；

2、访问控制

2.1 禁止产生越权访问漏洞；

2.2 禁止产生未授权的访问漏洞；

2.3 禁止产生目录遍历漏洞；

2.4 传递参数的页面须使用身份鉴别的令牌机制，Token可以由访问来源、访问对象、时间戳、有效期、随机数等信息组成；

2.5 对于需要登录后才能访问的页面资源，系统应支持防重放攻击，避免未授权的第三方伪造类似页面请求后成功获取页面资源；

2.6 禁止注入漏洞，含SQL注入、LDAP注入、xpath注入等；

2.7 开放接口安全

2.7.1 接口以HTTP（S）方式开放；

2.7.2 设计接口需要有身份认证，对来源授权，只允许授权的IP访问；

2.7.3 关键的（功能）接口调用需要有日志记录；

2.7.4 参数传递需要做签名，签名需要有失效性，建议失效时间：<=30分钟；

2.8 文件上传

2.8.1 禁止存放上传文件的目录拥有执行的权限；

2.8.2 上传文件类型限制，限制规则必须在服务器段校验，必须使用白名单进行限制，禁止使用黑名单限制规则；

2.8.3 存在图片上传时，对图片文件的文件头进行符合性校验；

2.8.4 上传文件不可以存放在WEB服务器上，要存放到指定服务器；

2.9 组件的选择

 2.9.1 禁止使用有公开漏洞的中间件版本；

 2.9.2 数据库选择当前的主流版本，版本不能过低；

 2.9.3 禁止使用有公开漏洞的应用框架组件（如web报表、web编辑器、办公组件、论坛、项目管理、日志等）；

3、数据安全

3.1 区分高、中、低等风险级别参数的数据类别，按照不同风险等级设置不同操作界面，不同数据类别要可设置成不同的权限控制（用户密码表、个人信息表、权限配置表、系统操作日志属于高安全级别数据）；

3.2 需求敏感字段处理

3.2.1 数据传输方式应满足数据敏感程度的要求，如传输敏感数据，数据需加密或采用安全的传输协议与传输内容；敏感字段包括a. 真实姓名、b.身份证号、c.账户号、d.生日、e.手机号码、f.联系电话、g.联系地址、h.单位名称、i.密码、j.银行账号、k.信用卡号等；

3.2.2 显示敏感字段时，应屏蔽部分字节。在服务端进行屏蔽。身份证，银行帐号，信用卡号，密码不能明文在页面显示。

3.2.3 对敏感字段的操作（新增、维护、删除）应有日志或报表以供审核；

3.2.4 一般用户的批量数据浏览界面可屏蔽敏感数据的部分字节；

3.2.5 限制对敏感数据的复制功能。

3.3 批量数据操作

3.3.1 应对批量导入的数据长度和数据大小进行校验，防止数据长度过长或导入数据量过大等导致系统出现安全问题批量数据的导入应有校验；

3.3.2 严格控制复制、下载、打印、浏览、导入/导出批量数据的权限，对批量数据的任何操作都须产生报表或日志。

3.4 数据保存

3.4.1 存储在数据库表中的敏感数据须加密或混淆；

3.4.2 系统自动备份重要数据，并能设置备份的周期；

3.5 个人信息保护

3.5.1 涉及个人信息采集和保存的系统,须对个人信息主体提供个人信息的收集的授权同意功能；

3.5.2 涉及个人信息采集和保存的系统,须对个人信息主体提供个人信息的查询/更正/删除功能；

3.5.3 涉及个人信息采集和保存的系统,须对个人信息主体提供个人信息的撤回授权功能；

3.5.4 如业务需要收集个人信息,系统需发布个人隐私政策。

4、故障预警要求

4.1 提供系统故障、超过系统容量、数据出错合理性超出、操作失误权限不匹配等的报警功能，以对话框或禁止下一步操作的方式报警并记录在系统日志内。

5、日志和报表

5.1 应开启网页访问日志与数据库访问日志；

5.2 报表或日志文件不可修改或删除：存储在系统数据库的日志表数据不可以被应用系统中的任何用户（管理员、审计员、操作员）修改或删除；

5.3 系统应提供单独的日志审核界面（权限）供审计人员使用；须对任何日志文件进行保护；

5.4 系统产生的所有日志应按增量规则生成到服务器指定目录生成日志文件，或存储在系统数据库的日志表中。若使用数据库日志表的存储模式，系统应支持syslog协议，本地存储同时外发给存储到第三方日志服务器；

5.5 系统运行日志

5.5.1 需要能记录操作者、操作对象、时间、IP 、事件、操作结果（成功、失败）以及原因（如考虑性能，此功能可作为开关，必要时提供）；

5.5.2 系统模块组件状态变化，错误或警报的记录。

5.6 权限维护日志

5.6.1 维护员ID；维护日期、时间；

5.6.2 权限的新增、删除或变更的记录。

5.7 系统操作日志

5.7.1 用户ID；日期、时间和关键事件的细节，如登录或退出、增删改事件、点击访问数据；

5.7.2 系统提供用户的登录时长查询功能（对应要求1.15）；

5.7.3 记录单位时长内用户密码连续输错，导致账户被锁定的行为（对应要求1.10）；

5.7.4 成功的和被拒绝的对系统尝试访问的记录；

5.7.5 成功的和被拒绝的对敏感数据以及其他批量资源尝试访问的记录；

5.7.6 应对系统特殊权限，包括系统管理员、配置管理员、审计管理员的系统启停、账号建立和删除、权限分配和修改、日志查看等行为进行审计特权的使用。

5.7.7 系统字典维护、表单维护等配置参数维护与变更应记录。

四、商务要求：

交货期：210天内；

保修服务期：三年全保；

五、知识产权要求：

1. 在项目建设周期内，成交服务商利用医院提供的技术资料获得软件的知识产权及新的技术成果，归院方所有，院方拥有自主使用权。
2. 在项目建设周期内，院方利用成交服务商提交的技术服务工作成果所完成的新的技术成果，院方享有申请专利的权利及专利取得后的使用和有关利益，成交服务商为院方申请专利提供必要的材料和技术支持。
3. 软件维护期结束后，院方可根据实际需求修改系统、扩充功能，成交服务商应提供必要的协助配合。由此产生的具有实质性或创造性技术进步特征的新的技术成果，归院方所有。
4. 成交服务商在建设、维保该项目过程中所创造产生的有关本项目知识产权，包括但不限于软件著作权、技术专利权、设计方案图纸、各种说明书、测试数据资料、程序源代码以及其他技术文档，由院方依法所有。