

技术需求表（服务类）

制表时间： 年 月 日

项目名称	海量医疗数据安全应用研究		单价 (万元)	125	数量（项）	1	预算总金额 (万元)	125
需求类别	序号	需求名称	技术参数和需求内容					备注
符合性要求（*号指标或其他必须响应条款）	*1	服务要求	1. 提供开发服务。在院内现有的数据安全平台基础上，与甲方合作开发一套新型医疗数据安全应用平台，开发内容包含多源异构数据汇集与智能分类、数据安全运营与智能管控、数据脱敏与网络数据防泄漏四个模块和基础功能，用于支撑医疗大数据的全生命周期的安全治理和管控； 2. 平台及所有功能模块可互相联动，包括且不仅限于统一的登录管理，统一的数据源等； 3. 提供源代码服务。软件系统、源代码等资产归甲方，软件部署为B/S架构，系统中文界面； 4. 提供文档类服务。按甲方要求提供相应文档。平台开发完成后需配合甲方申请1个发明专利、4个软著。					本项目证明材料可为产品说明书、宣传彩页、技术白皮书、公司承诺函等之一
	2	其他符合性条款	1. 符合《中华人民共和国政府采购法》第22条资格。					
资格性要求（指对产品或企业投标资格的要求）	1	人员资格	项目经理不少于2人。实施团队人员不少于5人；					
	2	企业资格	1. 符合《中华人民共和国政府采购法》第22条资格。					
	3	其他资格性条款	无					
	*1	项目经理	本项目采用A/B角项目经理					
	2	项目经理具备资质	2.1项目经理1	•1. 项目经理应具备10年以上网络安全行业工作经验，须具备本科及以上学历 •2. 项目经理应掌握项目管理体系知识，同时具备项目管理PMP证书 •3. 项目经理应掌握网络安全和数据安全知识，同时具备信息安全专业人员CISP证书和数据安全治理专业人员CISP-DSG认证 •4. 项目经理应掌握安全运维和风险管理能力，同时具备ITIL4 Foundation认证和ISO27001 Foundation认证				

附件6

需求类别	序号	需求名称	技术参数和需求内容		备注
			2.2项目经理2	<ul style="list-style-type: none"><li>•1. 应具备5年以上网络安全行业工作经验，须具备本科及以上学历</li><li>•2. 项目经理应掌握项目管理体系知识，具备项目管理PMP证书和信息系统监理师</li><li>•3. 项目经理应掌握网络安全实操能力和数据安全知识，同时具备Security+认证和数据安全治理专业人员CISP-DSG认证</li></ul>	
	3	团队其他人员具备资质	产品厂商项目开发人员要求：本科或以上学历，要求不少于5人，每人同时具备CISP、ITIL、ISO27001证书；		
	4	开发服务方案			
			4.1.1数据来源管理	<p>1、支持对多类型多版本结构化和非结构化数据自动扫描发现；</p> <p>2、系统对待管理的数据库、文件服务器采用无需安装客户端的方式进行扫描；</p> <p>3、结构化数据自动发现：系统支持通过指定的IP段、端口段，自动扫描发现网络中的数据库资产，可自动识别数据库基础信息，包括但不限于数据库类型等信息，支持Oracle、SQL Server等常用数据库数据识别；</p> <p>4、非结构化数据：支持文件服务器非结构化数据扫描及识别，支持文件格式包含且不仅限于DICOM，HTML，TXT等；</p> <p>5、手动添加：支持手动添加数据源，按照数据源名称、数据源类型、主机及端口、库名/实例名、版本号、账号、密码等信息进行连接添加；</p> <p>6、数据域管理：支持以清单列表方式对数据源进行账号密码、数据源名称、部门、业务属性等扩展信息维护，支持数据特征、混合规则等多种识别规则配置；</p> <p>7、元数据管理：支持获取结构化数据库资产数据的schema、数据表、数据表中列等信息，支持获取非结构化资产数据的目录层级、文件路径、DICOM文件tag值、日志文件告警分类等信息；</p>	

## 附件6

需求类别	序号	需求名称	技术参数和需求内容		备注
	4.1	多源异构数据汇集与智能分类	4.1.2智能分类	<p>1、内置分类分级模板：包括但不限于基于业务属性、资产类型、安全防护级别等符合《信息安全技术 健康医疗数据安全指南(GB/T39725-2020)》、《信息安全技术 个人信息安全规范》(GB/T35273-2020)及其他医疗行业标准的分类分级模板；</p> <p>2、自定义分级分类规则：可通过配置规则算法形成自定义分级分类策略，对纳管数据资产进行自动分级分类，根据规则构建规则，结合业务需求灵活配置扫描策略；</p> <p>3、智能识别文本文件：针对内容提取关键词，自动生成策略用于绑定类别和级别进行分类分级；</p> <p>4、系统支持指定分级分类模板进行扫描、支持指定库进行扫描，支持指定目录进行扫描；</p> <p>5、支持对自动分类分级人工打标；</p> <p>6、支持按照分类分级模板标准目录结构，以清单列表方式查看分类分级结果，分类分级数据统计可视化展示内容包括且不仅限于资产类型、数据库类别及数量、文件类型及数量、分类及数量、分级及数量；</p> <p>7、支持按照文件或数据库的目录结构，查看分类分级结果；</p> <p>8、支持按照指定分类或级别查看数据分类分级结果；</p> <p>9、支持导出分类分级清单，数据安全运营与智能管控等模块可根据分类分级清单进行策略管控、脱敏等操作；</p> <p>· 10、支持对数据分类规则进行数据权重标记，数据权重可选范围至少包括：一般、重要、核心等；</p>	
			4.1.3数据敏感分级	<p>· 1、内置数据敏感级别模板：包括数据库表、数据库表的列、数据库和文件中患者姓名、门诊号、联系方式等信息；</p> <p>· 2、支持对数据库、文件服务器的敏感数据扫描，同时支持按照周期和立即执行等方式按照敏感级别模板进行数据扫描分级；</p> <p>· 3、支持基于数据分类分级对敏感结果查看，数据资产查看，进行细粒度分域分权，根据数据敏感级别和用户权限，分配不同的数据访问权限；</p> <p>· 4、敏感数据报告统计可视化展示内容包括但不限于：资产总数、数据库资产排行、敏感表排行、文件服务器敏感文件排行、文件服务器敏感类别排行等；</p> <p>· 5、分类分级报告统计可视化展示内容包括但不限于：数据类别分布、数据级别分布、涉敏资产排行、涉敏分类排行、敏感类型数量分布；</p> <p>· 6、按甲方指定范围的敏感数据进行过滤；</p>	
			4.1.4 任务管理	<p>1、支持数据扫描任务管理，包括但不限于执行、停止，同时支持查看任务执行进度及详情；</p> <p>2、对数据库扫描时，支持多实例同时下发，还可设置字段名、字段备注、数据库内容等识别方式，从而提高扫描的准确率；</p>	

附件6

需求类别	序号	需求名称	技术参数和需求内容		备注
技术性要求			4.2.1数据安全运营	1、支持对多源异构数据汇集与智能分类模块中数据资产进行安全运营和智能管控； *2、支持多种不同类型设备探针日志的采集，包括但不限于多源异构数据汇集与智能分类系统、网络数据防泄漏系统、数据库审计系统日志的采集； · 3、支持服务扫描和发现功能，通过扫描网络中的开放端口以及确定监听这些端口的服务。如主机IP、端口、主机操作系统、服务的类型等。并实现自动或手动将这些服务添加到数据库加固点； *4、支持对数据库访问进行持续监测，根据配置的数据库审计策略，对数据库的风险操作进行自动化的告警，提升数据库的访问监测； 5、支持将相关日志上报到数据安全运营与智能管控平台进行数据汇聚；	
			4.2.2态势分析	1、支持数据资产态势展示，便于快速了解当前数据资产状态，提供数据资产视图、敏感数据资产视图、数据分级分类视图、数据资产热度视图等； 2、支持数据风险的全景视图展示，包括数据安全事件概述视图、数据安全事件量视图、数据安全风险趋势视图、数据资产流向视图、应用行为视图等；	
			4.2.3安全策略中心	1、支持数据安全管控全景图； 2、支持整体安全策略管理及展示，包括但不限于数据分类策略、数据分级策略、数据扫描特征、数据扫描组合特征等 *3、支持查询策略的导出，并支持多种导出模式，包含CSV/TXT/XLS等格式 4、支持数据安全规范库展示，列表至少包括：标准ID、标准名称、标准号、录入人员、生效时间、标准状态； 5、支持预览数据安全规范详情，至少包括：简要内容、明细列表，其中明细列表至少包括：明细项编号、明细项名称、明细项详细内容、明细项解读； 6、支持对数据安全规范标准进行批量生效、批量注销、批量删除操作，支持单个添加数据安全规范标准，并对单个数据安全标准进行预览、编辑、生效、注销、删除等操作，支持导出数据安全规范标准库； 7、支持数据分类列表呈现，至少包括：数据分类、备注、数据等级、策略状态等信息，并支持列表上直接展开呈现子集数据分类信息； 8、支持数据分级列表呈现，至少包括：数据等级、优先级、备注、安全规范、策略状态等信息； 9、支持数据分类分级规则管理功能，至少包括：全量下发、批量生效、批量失效、批量删除等批处理操作，同时支持对指定数据分类分级规则进行新增、编辑、注销、生效、删除等操作，对数据分类分级规则进行灵活管理； · 10、支持对数据分类规则进行数据权重标记，数据权重可选范围至少包括：一般、重要、核心等； 11、支持预置数据分类分级检测规则；	

附件6

需求类别	序号	需求名称	技术参数和需求内容		备注
	4.2	数据安全运营与智能管控	4.2.4安全扫描特征管理	<p>1、支持扫描特征（单特征和组合特征）管理功能，至少包括：导出、全量下发、批量生效、批量注销、批量删除等操作，同时支持对指定扫描特征进行新增、编辑、注销、生效、删除等操作，对扫描特征进行灵活管理；</p> <p>· 2、支持添加扫描特征（单特征和组合特征）时，关联对应的分类分级信息，同时可对目标范围、命中率、识别方式、识别内容、识别长度等进行精细化配置，并支持自定义对应的防护建议，为数据分类分级的落实提供支撑；</p> <p>3、支持批量导入扫描特征（单特征和组合特征），可下载模板并填写必填信息后上传至平台，快速梳理扫描特征；</p> <p>4、支持预览扫描特征（单特征和组合特征），查看策略下发数据资产梳理组件、文件资产梳理组件状态；</p>	
			4.2.5数据安全分析	<p>*1、支持网络防泄漏安全事件列表展示，能够详细地展示泄漏事件信息，至少包含事件ID、发送者、用户、部门、违规策略、泄漏时间、泄露方式、处置方式、事件状态、邮件主题、邮件正文、邮件附件列表、敏感文件列表、条件名称、敏感内容快照、敏感数据所在位置、匹配度、留存位置等详细信息，支持快速检索；</p> <p>2、支持网络防泄漏安全事件从事件趋势、泄露方式、策略名称、部门泄露TOP等维度统计分析，并支持自定义时间进行统一检索分析；</p> <p>3、支持数据库访问安全事件列表展示，能够详细展示至少包括发生时间、业务用户名、操作终端主机名及IP地址、终端工具名称、服务器端主机名及IP地址、数据库名、表名、SQL语句、响应时间、返回结果、命中策略、事件等级等关键信息；</p> <p>4、支持数据库访问安全事件从事件趋势、数据库、业务用户名、策略名称、风险等级等维度统计分析，并支持自定义时间进行统一检索分析；</p>	
			4.2.6安全报告中心	<p>1、对当前业务环境中的数据资产、账号行为、应用行为等进行审计管理；</p> <p>2、支持数据资产报告，提供分类、分级等多维度分析数据资产；</p> <p>3、支持账号行为风险分析报告，提供账号风险概览、高危账号分析、账号风险列表等；</p> <p>4、支持应用行为风险分析报告，提供应用风险概览、应用风险行为分布、应用风险列表等；</p> <p>· 5、支持网络防泄漏风险分析报告，提供网络防泄漏风险分析总览、策略规则分布、高危用户分布、风险列表等；</p> <p>· 6、支持数据库安全风险分析报告，提供数据库安全风险概览、风险等级分布、策略规则分布、风险列表等；</p>	

## 附件6

需求类别	序号	需求名称	技术参数和需求内容		备注
			4.2.7分域分权	<p>1、支持预置角色信息，至少包括：超级管理员、单位管理员、部门管理员、业务系统管理，预置角色支持预览，不可删除、编辑；</p> <p>2、支持添加角色，支持配置菜单模块及子菜单的查看和配置权限，配置代表可进行编辑、删除、新增操作，查看代表仅支持查看不可修改；</p> <p>3、支持预置admin用户，角色为超级管理员，组织机构为全部组织机构，支持树形结构筛选查看用户信息；</p> <p>· 4、支持添加用户，配置账号名、角色、用户密码、邮箱地址、机构结构等信息，可使用创建用户登录系统，资产清单、日志检索、风险列表、订阅管理等页面仅可查看当前用户有权限机构的数据，实现用户权限限制；</p>	
	4.3	数据脱敏模块	4.3.1脱敏库支持	<p>1、支持Oracle、Sql Server、Sybase、Mysql等关系型数据库；</p> <p>2、支持数据仓库脱敏；</p> <p>3、支持hive、Hbase等大数据平台脱敏；</p> <p>*4、支持读取txt、csv、excel、xml、DICOM等医疗影像文件；</p> <p>5、数据脱敏过程不落地，无需额外存储中间数据；</p> <p>6、支持源库到目标库脱敏（包含支持同库脱敏）、数据库到文件脱敏、文件到文件脱敏（包括FTP和SFTP方式）、文件到数据库脱敏；</p> <p>*7、支持主流关系型数据库（Oracle、DB2、SQL Server、Mysql）之间的异构脱敏、关系型数据库（Oracle、DB2、SQL Server、Mysql）与大数据平台之间的异构脱敏；</p>	
			4.3.2脱敏规则	<p>1、支持通过抽样的方式进行敏感数据发现，可自定义发现规则、抽样比例和匹配率。包括随机化、模糊化、置空、乱序排列、重复值屏蔽、随机替换、特定规则替换、身份证号脱敏、姓名脱敏、地址脱敏、电话脱敏、邮箱脱敏等算法，剔除或个人信息等敏感数据；</p> <p>2、支持自动检测源数据库DDL的变动，识别增量的新数据表的敏感信息。</p> <p>3、支持混合类型的敏感数据发现；</p> <p>4、支持针对影像图片、诊断记录等拥有一定规律的半结构化文本敏感发现，自动发现文本中的相关敏感信息；</p> <p>5、支持数据脱敏后保持原有数据特征、关联性、一致性（同一库、不同库）；</p>	

## 附件6

需求类别	序号	需求名称	技术参数和需求内容	备注
	4.4	网络数据防泄漏模块	*1、支持关键字监测、正则表达式监测、数据标识符监测、数据指纹监测、文件属性监测内容识别；支持识别网络协议：HTTP协议、HTTPS协议、FTP协议、SMTP协议、POP3协议、IMAP协议； 2、支持策略批量导入导出功能； · 3、具备图章识别能力，能够发现常见的文档、图片中是否携带有图章，并可以根据图章中的文字识别图章类型； · 4、对于word、ppt等嵌套文件和zip、rar等常见压缩文件能够判断文件嵌套或压缩的深度，深度至少识别出100层；同时，也可以将每个被嵌套的文件进行单独的内容识别，判断要识别的内容是否都在一个被嵌套文件中，还是分散在多个嵌套文件中； · 5、能够按excel文件中的每个sheet页进行内容识别，能够限定比如身份证号码、手机号码需要同时出现在同个sheet页中； · 6、能够通过代理方式，提供web访问、邮件收发、文件传输服务，并对传输的过程进行控制，支持源地址白名单和目的地址白名单； · 7、系统能够对内部的web系统、邮件系统提供代理服务，对发送到web系统、邮件系统和从web系统、邮件系统下载的数据、文件进行识别和防护； 8、支持对发生的泄漏事件进行告警和阻止的能力，支持邮件、SYSLOG等方式；	
	*5	售后服务	1 数据不出院，一切部署、运维工作必须现场实施，项目所有实施过程本地完成，不接受任何远程服务方式； 2 服务期内出现紧急故障情况，公司响应时间≤30分钟，到达现场时间≤2小时，解决问题时间≤4个小时； 3系统实施部署期间驻地工程师≥1人；	
	*6	验收考核办法	完成"服务要求"中所有项目同时开发系统需通过具有CMA、CNAS资质的第三方软件测评机构的测试，出具测评报告	
	*7	服务时间	合同签订后20日内完成整体项目开发服务（包含节假日）。	
	8	技术力量	· 1. 产品厂商具备相应数据安全项目经验及能力，提供不少于3个数据安全类产品合同，金额在100万以上。 *2. 产品厂商需具备软件成熟度模型认证CMMI-5级证书，提供有效证书复印件； · 3. 具备中国信息安全测评中心—信息安全服务资质（安全工程类二级及以上）证书； · 4. 服务商具有中国网络安全审查技术与认证中心CCRC信息安全应急处理一级资质(提供证书资质复印件，并加盖公章) · 5. 服务商具有中国网络安全审查技术与认证中心CCRC信息安全风险评估一级资质(提供证书资质复印件，并加盖公章)	

附件6

需求类别	序号	需求名称	技术参数和需求内容	备注
说明：1. 加注“*”号的技术指标为关键指标，≥1项未达到招标文件要求，即做废标处理 2. 加注“●”号的技术指标为重要指标 3. 加注“*”、“●”号的技术指标均需投标企业提供证明材料				