**防统方系统升级改造用户需求书**

### 1.1项目描述

### 为贯彻落实国家卫健委《关于加强医疗卫生机构统方管理的规定》(国卫纠发〔2014〕1号)的通知,为进一步规范医疗卫生服务行为，加强行业作风建设，严禁不正当商业目的统方，维护正常工作秩序。非正常统方行为作为药耗回扣利益链条中的重要环节，既违反了《卫生部八项行业纪律》、《医疗机构工作人员廉洁从业九项准则》，同时触犯了中华人民共和国刑法第285条第2款，将构成非法获取计算机信息系统数据、非法控制、计算机信息系统罪,破坏了医疗机构良好的公众形象，降低了医疗机构的社会满意度,这种行为严重影响医院及医疗机构的社会形象，因此医院需要部署控制统方的系统，并保证审查数据保存180天以上。我院原防统方系统软硬件版本过旧，无法满足新形势下的智慧医院、清廉医院建设要求，现需对防统方系统进行升级改造。

|  |  |  |  |
| --- | --- | --- | --- |
| **名称** | **数量** | **防护区域** | **预算金额** |
| 防统方系统 | 1套 | 用户指定地点 |  |

### 1.2技术参数

|  |  |  |
| --- | --- | --- |
| **序号** | **功能模块** | **参数要求** |
| **1** | **系统基本模块** | 1. 管理、审计用户权限分开，相应权限的用户只能查看、管理相应的系统功能，责任明确。
2. ▲产品为专业防统方系统，提供“防统方系统”的《软件著作权登记证书》，提供加盖公章的证书复印件。
3. ▲支持多院区、一院两区等情况分布部署及监控。

4.系统应具备对应用程序、数据库访问者、访问者IP地址等统计功能。并能提供按月统计每天的数据接口流量，统计出每月最大流量和最小流量的日期、终端、应用程序等，且形成趋势图。5.支持多种部署方式（串接/并接）都能够阻止客户端进行疑似的统方行为。6.系统支持采用旁路部署方式，不需要更改现有网络结构、服务器相关配置，系统运行不得影响现有网络和业务的正常运行。系统应能独立完成审计数据采集，不依赖于数据库自身审计日志系统，不得在现有服务器上安装可能带来风险的程序。7.系统确保最小报警监控时间间隔为5秒，保证统方事件的及时告警。8.系统的时间可以和关键服务器中的数据库的时间进行同步，确保记录时间的一致性。9.支持加密方式的数据库连接信息分析，提供产品截图。10.支持对Oracle、MS-SQL、DB2、MYSQL、CACHE DB、POSTGRESQL和Sybase 等数据库提供自动化评估、审计和保护功能,可审计的数据库或集群数量不少于20个，并且支持单家医疗机构多种类型数据库并存的信息系统。11.具备用户行为记录功能，记录用户所有操作（业务访问、系统维护、策略配置等）。12.系统从业务流程角度入手，结合核心数据特征，形成高度集成的“事前+事中+事后”数据防护手段。13.系统配置文件支持导入、导出。系统支持在线升级功能，通过厂家发布的升级包可在线对系统进行软件升级和规则库升级。14.系统为软硬一体机，支持千兆以上网络环境及大概至少500个客户端同时并发的监控，应达到每秒50000个以上的事务处理能力。15.采用B/S架构（兼容不同种类浏览器），提供中文WEB管理界面以便于管理。并应可以根据不同的安全级别采用不同的实时告警响应方式，包括记录、消息、鸣音、邮件等，并能支持短信平台。16.审计数据归档能永久保存，并支持外接存储设备进行备份。数据进行加密保管，只能通过专门工具进行恢复和查询浏览。支持数据自动备份、手动备份且可修改备份策略。 |
| 2 | **防统方模块** | 1. 能够出具针对纪委、监察室相关人员使用的防统方审计报告（支持每天或多天生成统方审计报告，报告需简单明了，且具有主动将所有的计算机语言翻译成通俗易懂的自然语言的系统机制，支持将整条SQL语句翻译成中文，帮助医院建立基于内部网络的党风廉政、廉洁警示、院内敏感职权使用的防控专网，支持对接廉政风险防控系统。
2. ▲内置防统方知识库，且具有独立自主统方学习功能，帮助医院深化党风廉政建设和反腐败工作,规范药品统计权限管理。支持对接医院智慧党建平台进行管理。
3. ▲系统支持虚拟化、虚拟云等网络环境的数据审计功能，准确定位统方行为。
4. ▲系统可针对耗材、高值耗材、SPD、检验试剂、合理用药、互联网医院等医院新的信息化系统进行审计,提供“**防统方系统**”的《中国国家信息安全产品认证证书》。所提供的证书需与投标产品、软件著作权名称、型号、版本号保持一致。
5. 能够获取客户端访问数据库的应用程序。根据客户端应用程序名单，实时阻止非法客户端程序或伪装正常客户端程序对关键服务器的访问。
6. 可以精确定位可疑对象的物理位置（记录操作人员工号、操作类型、IP地址、客户端工具以及存放路径、操作系统用户名、主机名、MAC地址、SQL语句和操作的时间等关键信息）。
7. 可以对某统方行为的所有操作以及操作结果关联起来，以报表的形式呈现给使用部门，便于使用部门分析和追溯统方事件。
8. ▲对于系统捕捉的非法统方行为，需要在医院年度医德医风考评中体现“一票否决”，支持与医德医风系统对接联动，提供加盖公章的证书复印件。
9. ▲发现统方操作后，可以对应相应药品厂家，对该厂商、药代表进行重点监控。
10. 统方白名单权限的设置，可对授权统方行为的操作人员工号、操作类型、IP地址、客户端工具、操作系统用户名、主机名、MAC地址、SQL语句和操作的时间范围等条件进行设置，只有通过了授权和验证才可以获得统方权限。
11. ▲系统根据操作行为归类信息集中医生的身份要素特征及操作要素特征，结合构建的待测医院对应的医生身份操作关联模型，得到相应医生的统计操作行为对应的模型关联系数，并识别医生的统方风险行为信息。该功能是防统方系统的核心功能，需提供国家专利局颁布的一种基于互联网的医疗数据安全监测系统及方法的《发明专利证书》，提供加盖公章的证书复印件。
 |
| 3 | **数据审计模块** | 1. 主动/被动方式监控关键服务器的开放端口，提供扫描现有应用系统的漏洞。
2. 能够对数据库操作的结果进行解析，审计内容包含数据库操作结果，并能实现回放功能。
3. 支持医院各生产系统中财务数据、病人资料、药品信息、医院资产等核心数据的审计监控。
4. ▲用户可以根据需要自定义规则，并能根据设定的条件产生审计报告。能对审计结果进行多条件组合查询，比如按下列条件查询：IP地址、MAC地址、表名、字段名、操作方式（可单独或者多选某种数据库操作）、计算机名、数据库名、程序名（可单独或者多选某个应用程序）等。并就能支持按关键词进行模糊查询。查询结果应支持多种格式(excel、pdf、txt等)导出。
5. ▲支持医院各生产系统中财务数据、病人资料、药品信息、医院资产等核心数据的操作审计监控。
6. 支持指定非关注策略，系统将非关注的内容进行过滤，不进行记录，降低存储空间和无用信息的堆砌。策略因子包括：数据库操作来源IP地址、数据库登录用户名称、数据库操作源程序名称、数据库操作源终端名称、数据库操作源终端用户名称、SQL操作语句（DDL、DML、DCL）、数据库表组（表、列）等。
7. 支持医院信息管理系统多层结构，提供全方位的三层（应用层、中间层、数据库层）的访问审计，三层关联支持自动关联，提升关联准确度和审计人员追踪索源难度，同时需要支持手动关联，可以直接追踪到前端业务的操作人员IP地址、MAC地址和用户。
8. 提供数据库登录用户名称异常探测、数据库操作源终端异常探测、数据库操作源程序名称异常探测、数据库操作源终端用户名称异常探测，可设定异常黑白名单，对客户端地址、客户端程序、数据库账号、客户端用户名以及执行结果等异常的行为进行异常告警，支持自主学习能力。
9. 系统能支持多个网段客户端对数据库操作行为的会话审计，能够对各种访问数据的途径进行监控和设计，可以跟踪审计某时间、某IP、某计算机名、某用户对数据库服务器进行了该类操作，具有可疑对象定位功能，可以精确定位可疑对象的物理位置。
10. 产品从审计主体、审计客体、日志格式、规则分析能力、报表、告警、存储等模块完全按照等级保护基本要求和测评要求设计研制。
11. 系统应能支持对数据库SQL操作语句的详细审计，可以分析出每条语句的操作方式、表名、存储过程名、详细操作内容，执行时长、操作成功/失败，受影响行数，关联表与关联表数等字段信息，可审计并还原SQL操作语句。
12. 可根据SQL执行的时间长短设定规则，如命令执行时长超过30秒进行告警；可根据返回记录数多少设定规则，如SQL操作返回的记录数或受影响的行数大于等于10000行时进行告警。
13. 支持超长操作语句审计，针对传统型数据库，支持 3万字节的审计而不截断，针对 Cache数据库，支持60万字节长度不截断。
14. 支持对双向数据包的解析、识别及还原，不仅对数据库操作请求进行实时监控，而且还可对数据库系统返回结果进行完整的还原，根据统方行为的特征实时告警，提供产品截图。
 |
| 4 | **抗菌药物试剂及耗材分析模块** | 1. ▲支持对指定时间内全院抗菌药物、试剂及耗材的品种、剂型、规格、使用量、使用金额，使用量和使用金额分别排名前N位的品种进行分析，自动生成报表）。
2. ▲支持针对医院使用的抗菌药物、试剂和耗材进行全方位跟踪，提供条件筛选模糊查询和精确查询，系统能实时对抗菌药物、试剂和耗材的统计进行告警。
 |
| 5 | **告警模块** | 可根据用户自定义规则实时发出手机短信通知和邮件提醒等多种方式的告警信息，并支持配备相应的告警信息发送设备。 |
| 6 | **移动端展示** | ▲可以通过移动端收发报警并展示，报表查询，设备状态查看，可以在移动端上进行报备审批等。具有防统方系统移动端管理的《软件著作权登记证书》，提供加盖公章的证书复印件。 |
| 7 | **历史数据可溯源** | ▲对于升级前防统方系统数据，可通过数据库接口以及数据转换工具汇聚展现。方便使用者对历史数据进行查看访问。 |
| 8 | **配置需求** | 支持以下配置：吞吐量：≥10GbpsSQL事务数/秒：≥100,000接口：≥10/100/1000M自适应电口 \*6万兆光纤模块≥ 2个存储容量：≥16TB，存储周期不少于180天处理器：≥Intel 系列（CPU具体型号主频不低于3.7GHz，CPU线程≥12）内存：≥32G |

### 1.3 服务要求

1. ★系统免费升级与维护期为叁年，实施上线、维护工作必须由原厂厂家完成；必须在合同签订后30个工作日内完成系统开发和初验，初验后开始试运行并在试运行30个工作日后进行最终验收。
2. 供应商需提供免费维护期后升级和维护的费用标准。
3. 提供7\*24小时电话、现场的维护、软件升级服务；每季度至少提供一次巡检及协助报告分析服务。
4. 当收到医院的报修要求时，若2小时内电话无法解决，4小时内到达现场进行维护，48小时内解决完毕。

### 1.4 接口要求

1.▲中标人必须与采购方原有防统方系统实现无缝联接，兼容采购方原有系统软件和数据库，确保系统的使用。

2.▲中标人必须与采购方原有防统方设备使用统一（兼容）的操作系统、统一的后台数据库及统一的系统接口标准与网络协议。