**云南省精神病医院**

**传染病智能监测预警项目建设方案**

目录

一、 项目概况 2

二、 建设背景 2

三、 现状及需求分析 3

四、 建设目标 4

五、 主要功能要求 5

六、 系统集成及服务 13

## 项目概况

项目名称：云南省精神病医院传染病智能监测预警项目服务器采购

1、建设单位：云南省精神病医院。

2、项目预算：7.5万元。

3、建设内容：国家传染病智能监测预警前置软件服务器，含配套设施设备、系统集成及服务等。

4、项目工期：签订合同后60日历天内完成。

5、项目实施地点：云南省精神病医院。

## 建设背景

为落实2020年6月2日习近平总书记在专家学者座谈会上指出的“建立智慧化预警多点触发机制，健全多渠道监测预警机制”重要讲话精神，2023年1月国家疾病预防控制局印发了《加快建设完善省统筹区域传染病监测预警与应急指挥平台实施方案》的通知，提出构建全国一盘棋、纵向一体化传染病智慧监测预警与应急指挥信息平台的总体架构和重点应用信息系统的具体任务。

2024年3月，国家疾控局印发了《关于做好国家传染病智能监测预警前置软件服务器软硬件环境配置》，云南省疾控预防控制局印发了《关于做好国家传染病智能监测预警前置软件服务器软硬件环境配置的通知》的通知。按国家和省卫生健康委要求，2024年有部署任务的单位需在 6月 30日前完成本单位传染病智能监测预警前置软件服务器软硬件环境配置，2025年前全市二级及以上传染病网络直报公立医疗机构智能监测预警集成部署应用率不低于 50%。

按照《昆卫便签关于按时间节点加快推进国家传染病智能监测预警前置软件部署工作的通知》， 为加快推进传染病智能监测预警前置软件服务器软硬件环境配置工作，确保传染病智能监测预警与应急指挥能力提升项目任务按要求完成，故建设云南省精神病医院传染病智能监测预警项目。为确保前置软件的安全运行，必须确保其部署环境的稳固性与数据存储的安全性。为此，应采用符合国家相关法律法规规定的数字证书及相应的密码产品或服务，以保障数据在存储和传输过程中的完整性、加密性和不可否认性。在此过程中，所选用的CA证书应当能够与现行的传染病网络直报系统所使用的CA证书实现兼容与互认。

## 现状及需求分析

全国一体化传染病监测系统总体架构包含“国家数据集成服务平台”和“国家传染病智能监测预警前置软件”两个部分，其中“国家传染病智能监测预警前置软件”需部署在医疗机构前置服务器，具备与“国家数据集成服务平台”进行数据交换功能，同时支持与“省统筹监测预警平台”等其他平台提供数据服务，保证传染病数据采集和存储安全。

随着《密码法》《数据安全法》《个人信息保护法》以及《商用密码管理条例》等文件的落地实施，信息系统应采用密码技术，建立密码应用保障系统，保障网络和数据安全，且采用的密码技术应符合法律法规的规定要求，确保密码应用的合规性、正确性、有效性。

（1）医院前置系统安全需求

医院前置系统通过接入院内HIS系统及医生填报等方式，汇集了大量传染病数据。医院前置系统是医院与上级单位上报的核心中转枢纽，疾控数据一旦泄露将对个人、医院及社会造成严重危害，采用必要的技术手段保障医院前置疾控数据的真实性、完整性及机密性显得尤为重要。

（2）医生终端数据上报安全需求

本项目为方便医生实时在移动终端填报疾控数据，国家局中心端面向医生开放了登录填报的模式，在带来业务便捷性的同时，移动终端安全不容忽视，需要有效解决移动端医生网络身份真实性以及移动终端数据安全传输性需求。

（3）服务器的资质资格及性能需求

基于《云南省卫生健康委办公室关于转发监测预警与应急指挥能力提升项目工作任务清单的通知》文件要求，针对有部署任务的全省二级及以上医院要按照《国家传染病智能监测预警前置软件服务器软硬件环境配置要求(试行)》中服务器配置要求、网络配置要求和安全相关配置要求准备软硬件资源，其中带宽要求根据云南省的实际情况，调整为医疗机构需要具备至少一个固定互联网IP地址，配备符合商用密码以及信创标准的IPSECVPN网关设备，吞吐量>1Gbps。

## 建设目标

根据云南省疾控《云南省疾控预防控制局关于做好国家传染病智能监测预警前置软件服务器软硬件环境配置的通知》云疾控规财函[2024]1号文的要求，需要在医院外网侧部署支持符合商用密码以及信创标准的IPsec VPN网关设备，实现智能监测预警系统软件的数据上报，防止疾控数据泄露的风险，确保医院传染病智能监测预警前置系统的数据安全及上报工作。

（1）具体功能及业务目标

符合《国家传染病智能监测预警前置软件服务器软硬件环境配置要求(试行)》的配置要求。服务器满足《国家传染病智能监测预警前置软件服务器软硬件环境配置要求(试行)》的配置要求，CPU位于《安全可靠测评结果公告(2023年第1号)》，兼容麒麟、欧拉、统信等国产操作系统，支持部署OpenGauss数据库。

（2）符合商用密码和信创标识

IPSec VPN网关为国产化设备，CPU采用国产自研CPU，操作系统采用国产操作系统。设备配备硬件密码卡，支持SM1、SM2、SM3、SM4算法。

（3）用户身份鉴别

安全网关提供web认证、证书认证、802.1X认证、POP3认证手段，提供本地认证服务器功能，并可与第三方RADIUS、TACACS+、LDAP、Active Directory认证服务器进行联动，同步用户认证信息。通过安全网关提供的用户认证功能，配合第三方用户认证服务器，实现针对用户的身份鉴别，保障接入网络的用户的真实性得到验证。

（4）动态流量调度

通过安全网关提供的流量管理功能，可以实现基于业务、用户的维度实现对重点业务的带宽资源保障，对剩余带宽的动态分配，对每用户下发带宽配额。在网络资源有限的情况下，保障重点业务的服务可靠性。

（5）管理员三权分立

对于管理安全网关的运维人员，实行三权分立。通过安全管理员、审计管理员、系统管理员权限划分及管理前的身份鉴别来保证安全网关的合理规范运维及密钥安全。

管理员的身份鉴别可采用双因素认证，基于SM2证书的方式，将证书放入智能电子钥匙中。管理员登录管理设备必须匹配上管理员身份的证书及其对应的用户名口令，方可登录管理安全网关。满足等级保护及密码测评要求。

（6）兼容性

通过安全网关提供的经国家密码管理部门核准的国密协商模式进行IPSec VPN方式组网，可保证对通信双方进行认证，可防截获、防假冒和防重用，保证传输过程中鉴别信息的机密性和网络设备实体身份的真实性，标准协议的对接方式，解决了不同厂商设备带来的对接壁垒。

## 主要功能要求

### 1、应用场景及网络架构



（1）在医院数据中心出口部署安全网关，在专线或互联网环境中建立国密协商模式的IPSec VPN隧道。

（2）院内部署前置服务器，用于安装国家传染病智能监测预警前置软件，保障数据能够及时收集、上报。

### 2、建设方案

（1）总体思路

采用国产密码算法和技术，第三方CA机构颁发的数字证书标识各相关医疗机构在数据监测采集时的网络数字身份，确保身份真实；采用数字信封技术，对采集的敏感数据进行签名、加密，确保敏感数据不被篡改和泄露。利用数字证书和数字信封技术的优势就是实现安全、高效的加密密钥管理，为医院（含移动端用户）颁发第三方合法CA机构的数字证书即可，无需管理每次采集都需要频繁使用的加密密钥，而数字证书的密钥安全性由第三方合法CA机构负责。所选用的CA证书应当能够与现行的传染病网络直报系统所使用的CA证书实现兼容与互认。

（2）方案设计

保障医院传染病数据安全采集，在全国二级及以上医疗机构和统一使用区域平台开展诊疗服务的医疗机构发放标识其身份的单位数字证书；为医生颁发移动证书，用于在移动终端传染病数据上报过程中的身份鉴别及数据安全保护。



1）医院前置向国家局及省级疾控数据上报

面向传染病智能监测预警前置软件服务器端颁发单位数字证书，用于解决疾控数据上报来源的真实可信，利用电子签名技术防止数据被篡改，保障采集数据的完整性；同时，为医院前置提供数据加密服务，防止疾控数据泄露的风险。为解决医院前置数据密码产品应用的可靠性、稳定性，结合医院业务量情况，利旧现有密码机。

2）医院前置服务密码应用保护

采用国产自研CPU，整机物理核数≥64核，实现传染病智能监测预警前置软件的部署。该服务器面向互联网、分布式存储、云计算、大数据、企业业务等领域，具有高性能计算、大容量存储、低能耗、易管理、易部署等优点。



疾控医院前置加密机实现与疾控业务深度融合，支持数据加/解密运算、签名验签、完整性校验、密钥管理等服务，支持导入与现有传染病网络直报系统兼容互认的单位证书，能够有效确保医院前置数据的机密性、完整性与不可否认性，为医院前置服务提供更加安全可靠的应用环境。

3、**主要功能参数及要求**

|  |  |  |
| --- | --- | --- |
| **序号** | **名称** | **主要功能参数及要求** |
| 1 | 传染病智能监测预警前置软件服务器 | 1. 机型：2U机架式服务器，配置导轨；▲2. CPU：≥2颗国产自研CPU，单颗CPU核心数≥32核，单颗CPU主频≥2.6GHz；3. 内存：≥256GB 3200MHz DDR4 内存；4. 存储空间：≥2块1.92TB SATA SSD；5. 网口：≥1块四口千兆网卡，≥1块双口万兆网卡（带多模光模块），方便连接院内网络环境和外部网络；6.产品认证：提供第三方认证的MTBF时间≥40万小时证书及检测报告，投标产品须通过节能认证证书、环境认证证书并、3C认证证书，并提供证书复印件等；7.厂商资质：设备制造商应通过静电防护的标准认证 ANSI/ESD S20.20和IEC61340-5-1 两项认证标准，提供相关证书；为保障信息安全，并有效地降低用户隐私安全风险，要求产品厂商具备ISO27001信息安全管理体系认证、服务器领域ISO27701隐私信息管理体系认证，提供相关证书；8. 电源：配置≥2个900W热插拔冗余电源模块；9.GPU卡或NPU支持：可选配备GPU或NPU卡，便于提高AI算法计算速度和准确性，推荐传染病病例数量多的医院选配；10.操作系统：使用麒麟、欧拉、统信等国产操作系统的服务器版，包含安装授权许可的欧拉openEuler 22.03 LTS版本操作系统；11.数据库支持：配备OpenGauss或同等架构的数据库，服务器需支持运行此架构数据库，包含安装授权许可的OpenGauss 5.0.0 及以上版本数据库。▲12. 服务：3年原厂整机质保，3年原厂免费上门服务，提供服务承诺函加盖公章；13、为保障本次项目服务质量，要求设备厂商具备并提供NECAS售后服务体系完善程度认证证书，具备并提供售后服务标准CCCS符合客户联络中心服务认证和全国商品售后服务达标认证，产品服务符合信息技术服务运行维护标准并提供证书。▲14、提供国家传染病智能监测预警前置软件的安装实施服务，供应商提供承诺函；▲15、为保障系统的兼容性及适配性，要求本次采购服务器能够兼容医院现有密码机，供应商提供承诺函；▲16、使用CA证书完成服务器身份认证，CA证书应与现有传染病网络直报系统采用的CA证书兼容互认。 |

## 系统集成及服务

1. ▲包含项目所有产品的安装调试，包含openEuler操作系统，openGauss数据库安装，国家传染病智能监测预警前置软件安装服务，含系统重装修复服务。包含单位CA证书，用于标识医疗机构网络身份。满足医院传染病监测上报的业务和管理要求，支持与医院现有系统的数据对接，包括但不限于自主完成与HIS、电子病历和院感等系统的接口集成等费用，并自主完成各项传染病监测数据的匹配工作。
2. 有专业维修工程师及技术人员，能提供及时的技术支持及售后服务。设备发生故障、缺陷电话报修时，或接到采购人提出的技术服务要求后0.5小时内予以答复，如采购人有要求或必要时，应在1小时内到达现场免费维修和提供现场指导。接到维修通知后8小时仍不能现场解决问题时，应提供同一型号的备用机使用，直到设备恢复使用。

3、若在接到采购人提出的技术服务要求或维修通知后2小时内没有响应、拒绝或没有派员到达买方提供技术服务、修理或退换货物，采购人有权委托第三方对合同货物进行维修或提供技术服务，因此产生的相关费用由卖方承担。

4、质量保修期为验收合格之日起≥36个月。质量保修期内，免费提供合同货物的技术指导和维修服务。在合同货物保修期届满后，如果因合同货物硬件或软件的固有缺陷和瑕疵出现紧急故障和事故，中标人应在接到采购人通知之后2小时内到达现场。

5、提供本次项目中所有设备的优化、巡检、培训等服务，培训医院技术人员熟练使用设备。

6、质保期内，提供7\*24小时现场、远程支持服务；可对故障问题快速响应，并及时有效的分析处理，出具故障问题处理报告，做到故障不排除，技术服务人员不撤离，需要提供服务器原厂实施服务。同时，需每月及重大节假日前对设备进行巡检，保障设备的正常运行。

7、▲包含配套设施设备、网络、系统等整合实现闭环应用，包含必要的网络铺设、整改和集成等内容，满足昆卫便签关于印发《昆明市医疗机构国家传染病智能监测预警前置软件服务器软硬件环境配置实施方案（试行）》的通知等通知及文件的要求。项目为整体包干含税价，包含本次项目所有系统的安装、调试、培训、系统上线、系统集成等费用，交付标准为整体交付、集成并正常使用。

**备注：**

一、标注“▲”的均为重要参数，重要功能参数必须提供证明材料，证明材料包括：招标文件技术参数内明确要求提供的证明材料，未明确的可提供所投产品制造商提供的主要功能指标、参数及性能的详细说明书或系统截图。若响应文件中技术支持资料参数与技术规格偏离表应答不符或无上述技术支持资料，视为不响应该条技术参数。响应文件中涉及的重要技术参数需在投标文件所附的证明材料内图示标注。

二、功能参数中如出现产品名称、品牌型号，技术标准，功能等方面的描述均起到技术参照作用。供应商只需提供满足或优于相关功能参数即可，所列参数没有指向性。

三、验收时，对功能要求进行逐一测试验证，测试中发现虚假应标的行为将予以废标处理并保留对该供应商追究相关责任的权利，将依法依规提请相关主管部门进行处罚，并记入政府采购诚信档案等。