

第三部分技术需求书

1. 项目概述.....	2
1.1. 采购需求.....	2
1.2. 项目背景.....	2
2. 项目建设内容.....	2
3. 系统设计总体要求.....	3
3.1. 设计原则.....	3
4. 安全性设计要求.....	4
5. 新生儿疾病筛查管理系统安全升级建设详细内容.....	4
5.1. 通信传输整改.....	4
5.1.1. 传输完整性保护.....	4
5.1.2. 传输保密性保护.....	6
5.2. 安全审计整改.....	7
5.2.1. 系统安全审计措施.....	7
5.3. 数据保密性保护.....	8
5.3.1. 存储保密性保护.....	8
5.3.2. 传输保密性保护.....	8
6. 项目管理与组织及人员要求.....	10
6.1. 项目管理工作内容.....	10
6.2. 项目管理项目程序和制度要求.....	10
6.3. 项目管理实施方案要求.....	11
6.4. 系统管理及文档要求.....	11
6.5. 对项目团队人员角色和能力要求.....	12
6.5.1. 组织和人员的总体要求.....	12
6.5.2. 项目团队人员服务要求.....	12
6.6. 需求变更要求.....	13
7. 技术支持与售后服务.....	13
8. 知识产权要求.....	13

1. 项目概述

1.1. 采购需求

序号	项目名称	单位	数量	工期
1	新生儿疾病筛查管理系统安全升级技术服务	项	1	<p>本项目实施计划分两个阶段进行，请投标人根据阶段划分进一步细化成工作计划：</p> <p>第一阶段：合同签订后 3 个月内完成软件的开发测试工作，投入试运行；</p> <p>第二阶段：投入试运行后正常运行 1 个月，建立完善的系统运维体系，正式验收合格并投入使用。</p>

1.2. 项目背景

新生儿疾病筛查管理系统自 2008 年建设至今包括 4 个子系统和 2 个平台，分别是：新筛采血登记系统、区级质控管理系统、中心综合管理系统、实验室管理系统、新筛结果网上查询平台和短信发送平台，新生儿疾病筛查管理系统通过近几年的逐步完善各个功能模块，系统运行稳定、使用便捷。

2020 年 7 月新生儿疾病筛查管理系统经过专家评审定为系统安全等级保护三级，系统需要进行安全升级、技术改造，进一步完善系统中安全审计、通信传输、数据保密性保护等内容，以达到信息系统安全等级保护三级（以下简称等保三级）的相关要求。

2. 项目建设内容

(1) 新生儿疾病筛查管理系统各个子系统所交互的数据进行加密传输，重要数据加密存储，以满足等保三级的要求。

(2) 新生儿疾病筛查管理系统各个子系统、应用服务器及数据库服务器添加安全审计功能，以满足等保三级的要求；

(3) 新生儿疾病筛查管理系统各个子系统与中心应用服务器进行数据交互方式进行升级改造，以适应数据完整性和数据保密性的要求，以满足等保三级的要求；

3. 系统设计总体要求

3.1. 设计原则

1) 先进性

系统的设计和所采用的技术必须具备足够的前瞻性和先进性，考虑到医院业务发展所带来的海量数据处理，以满足医院业务运作对整个系统的要求。

2) 实时性

信息系统业务处理频繁、信息交换量较大，业务处理的速度直接关系到医院正常运作和经济效益，以及客户对医院的评价。在正常情况下，系统必须保证在大量业务运行良好的同时，拥有实时的快速响应能力，确保整个业务系统的畅通。

3) 安全性

满足等保三级的相关要求。在系统设计、实施阶段从多个方面充分考虑整个系统的安全性，并且系统中所有重要操作需留有记录，以便追根溯源。

4) 兼容性

支持 win7, win8, win10 等 32 位和 64 位操作系统。

5) 开发技术

业务平台采用 C/S 智能客户端模式，通过 WebService 提供数据服务，数据库使用的是 SQL Server。

6) 可扩展性

为适应不断发展的医疗业务，系统应具备良好的扩展性，开放性和移植性。

7) 易维护性

管理员可维护系统基础设置数据项，系统升级和日常维护只需要在云服务器进行即可。

8) 易用性

人机界面友好、直观、清楚、统一，可快速查询患者资料，达到简化操作、提高软件可用性、保证资料一致性的目的。

9) 可操作性

设计方案符合业务流程，切实可行。

4. 安全性设计要求

应按信息系统安全等级保护三级进行软件设计，并配合采购人做好等保测评相关工作。

5. 新生儿疾病筛查管理系统安全升级建设详细内容

5.1. 通信传输整改

以北京市政务云平台为基础，按照等保三级的要求，需要对新生儿疾病筛查管理系统各个子系统与新筛中心应用服务器进行数据交互方式进行改造升级，以适应数据完整性和数据保密性的要求。

5.1.1. 传输完整性保护

新生儿疾病筛查管理系统各个子系统与中心应用服务器通信时，需要采用数字签名的方式保证通信过程中数据的完整性，在通信过程中数据遭到篡改时，无法通过签名验证。

(1) 区级质控管理系统改造

区级质控管理系统在调用通信服务前，应采用数据校验签名算法计算需要传输的业务数据的校验码或数字签名，将校验码或是数字签名与业务数据传送至服务器，服务器系统应采用相应的校验算法或是数据签名算法，验证数据完整性，验证失败时应记录数据异常日志，同时系统返回异常信息，通信失败。

所改造内容包括用户登录、卡片上传、卡片信息验证、消息发送模块、卡片退回模块、追访管理模块、报表查询等与服务器通信的相关模块。

(2) 新筛中心综合管理系统改造

新筛中心综合管理系统在调用通信服务前,应采用数据校验签名算法计算需要传输的业务数据的校验码或数字签名,将校验码或是数字签名与业务数据传送至服务器,服务器系统应采用相应的校验算法或是数据签名算法,验证数据完整性,验证失败时应记录数据异常日志,同时系统返回异常信息,通信失败。

所改造内容包括用户登录、卡片扫描验证、卡片数据保存模块、卡片退回模块、门诊接收模块、追访管理模块、复诊管理模块、短信管理模块、电子病历管理模块、报表查询等与服务器通信的相关模块。

(3) 实验室管理系统改造

实验室管理系统在调用通信服务前,应采用数据校验签名算法计算需要传输的业务数据的校验码或数字签名,将校验码或是数字签名与业务数据传送至服务器,服务器系统应采用相应的校验算法或是数据签名算法,验证数据完整性,验证失败时应记录数据异常日志,同时系统返回异常信息,通信失败。

所改造内容包括用户登录、卡片扫描验证、实验批次管理模块、TSH 实验结果管理模块、PHE 实验结果管理模块、17-OHP 实验结果管理模块、MS/MS 实验结果管理模块、MS/MS 报告管理模块、数据核查模块、报表查询等与服务器通信的相关模块。

(4) 中心 web 服务改造

中心 web 服务在接收到通信数据后,应采用数据校验签名算法计算接收到的传输的业务数据的校验码或数字签名,并将计算结果与通信数据汇总的校验码或数字签名进行校验,保证数据完整性,验证失败时应记录数据异常日志,同时系统返回异常信息,通信失败。

所改造内容包括当前 Web 服务中的所有提供数据服务的 Web 方法。

(5) 实验室 web 服务改造

实验室 web 服务在接收到通信数据后,应采用数据校验签名算法计算接收到的传输的业务数据的校验码或数字签名,并将计算结果与通信数据汇总的校验码或数字签名进行校验,保证数据完整性,验证失败时应记录数据异常日志,同时

系统返回异常信息，通信失败。

所改造内容包括当前 Web 服务中的所有提供数据服务的 Web 方法。

5.1.2. 传输保密性保护

新生儿疾病筛查管理系统各个子系统与中心应用服务器通信时，应采用 HTTPS 协议通信或是采用自定义加密算法对数据加密后传输，以保证通信过程中数据的保密性。

(1) 区级质控管理系统改造

区级质控管理系统在调用通信服务前，应采用 HTTPS 协议通信或是采用对称加密技术对需要传输的业务数据进行加密，加密数据传送至服务器，服务器 web 服务应采用相应解密算法解密业务数据，解密成功后再保存至数据库。子系统的请求数据与服务器的响应数据均需要做加密解密处理，保证通信过程中传输的数据均为加密后数据。在传输过程中因数据篡改导致解密异常时，系统自动记录解密异常日志。

所改造内容包括用户登录、卡片上传、卡片信息验证、消息发送模块、卡片退回模块、追访管理模块、报表查询等与服务器通信的相关模块。

(2) 新筛中心综合管理系统改造

新筛中心综合管理系统在调用通信服务前，应采用 HTTPS 协议通信或是采用对称加密技术对需要传输的业务数据进行加密，加密数据传送至服务器，服务器 web 服务应采用相应解密算法解密业务数据，解密成功后再保存至数据库。子系统的请求数据与服务器的响应数据均需要做加密解密处理，保证通信过程中传输的数据均为加密后数据。在传输过程中因数据篡改导致解密异常时，系统自动记录解密异常日志。

所改造内容包括用户登录、卡片扫描验证、卡片数据保存模块、卡片退回模块、门诊接收模块、追访管理模块、复诊管理模块、短信管理模块、电子病历管理模块、报表查询等与服务器通信的相关模块。

(3) 实验室管理系统改造

实验室管理系统在调用通信服务前，应采用 HTTPS 协议通信或是采用对称加密技术对需要传输的业务数据进行加密，加密数据传送至服务器，服务器 web

服务应采用相应解密算法解密业务数据，解密成功后再保存至数据库。子系统的请求数据与服务器的响应数据均需要做加密解密处理，保证通信过程中传输的数据均为加密后数据。在传输过程中因数据篡改导致解密异常时，系统自动记录解密异常日志。

所改造内容包括用户登录、卡片扫描验证、实验批次管理模块、TSH 实验结果管理模块、PHE 实验结果管理模块、17-OHP 实验结果管理模块、MS/MS 实验结构管理模块、MS/MS 报告管理模块、数据核查模块、报表查询等与服务器通信的相关模块。

(4) 中心 web 服务改造

中心 web 服务在接收到加密的通信数据后，应采用 HTTPS 协议通信或是采用解密算法解密业务数据，再做相应的数据处理，解密失败时应记录数据异常日志，同时系统返回异常信息，通信失败。

所改造内容包括当前 Web 服务中的所有提供数据服务的方法。

(5) 实验室 web 服务改造

实验室 web 服务在接收到加密的通信数据后，应采用 HTTPS 协议通信或是采用解密算法解密业务数据，再做相应的数据处理，解密失败时应记录数据异常日志，同时系统返回异常信息，通信失败。

所改造内容包括当前 Web 服务中的所有提供数据服务的方法。

5.2. 安全审计整改

以北京市政务云平台为基础，按照等保三级的要求，需要对新生儿疾病筛查管理系统各个子系统、应用服务器及数据库服务器添加安全审计功能。

5.2.1. 系统安全审计措施

新生儿疾病筛查管理系统各个子系统需要添加审计模块，对用户操作行为进行日志记录、审计，审计范围不仅针对前端用户的操作、行为，也包括后台管理员、后台服务的操作日志。

(1) 区级质控管理系统

区级质控管理系统应记录全部的业务操作日志，包括用户登录日志、卡片扫

描登记日志、卡片上传日志、卡片信息验证日志、消息发送模块操作日志、卡片退回操作日志、追访管理操作日志、报表查询日志等。

(2) 新筛中心综合管理系统

新筛中心综合管理系统应记录全部的业务操作日志，包括用户登录日志、卡片扫描验证日志、卡片数据保存操作日志、卡片退回操作日志、门诊接收操作日志、追访管理操作日志、复诊操作日志、短信操作日志、电子病历管理中的全部用户操作日志、报表查询日志、卡片查询日志等。

(3) 实验室管理系统

实验室管理系统应记录全部的业务操作日志，包括用户登录日志、卡片扫描验证日志、实验批次管理操作日志、TSH 实验结果管理日志、PHE 实验结果管理日志、17-OHP 实验结果管理日志、MS/MS 实验结构管理日志、MS/MS 报告管理日志、数据核查日志、报表查询日志等。

5.3. 数据保密性保护

以北京市政务云平台为基础，按照等保三级的要求，需要对新生儿疾病筛查管理系统各个子系统所交互的重要数据采用有关部门批准的加密算法进行加密后存储和传输。

5.3.1. 存储保密性保护

新筛各个子系统涉及数据主要包括业务数据中手机号、联系地址等敏感信息必须加密后再存储至数据库。各个子系统在运行过程中产生的临时文件，如果涉及到业务数据，需要在本地缓冲的业务数据时，临时文件中的业务数据采用有关部门批准的加密算法加密后写入本地临时文件中；不需要在本地缓冲的文件，使用结束后及时删除文件。

5.3.2. 传输保密性保护

新生儿疾病筛查管理系统各个子系统与中心应用服务器通信时，数据包发送前采用对称加密技术，对业务数据进行加密，数据发送至应用服务器后采用反向

操作，进行数据解密，以保证通信过程中数据的保密性。

(1) 区级质控管理系统

区级质控管理系统在调用通信服务前，应采用对称加密技术对需要传输的业务数据进行加密，加密数据传送至服务器，服务器 web 服务应采用相应解密算法解密业务数据，解密成功后再保存至数据库。子系统的请求数据与服务器的响应数据均需要做加密解密处理，保证通信过程中传输的数据均为加密后数据。在传输过程中因数据篡改导致解密异常时，系统自动记录解密异常日志。

所改造内容包括用户登录、卡片上传、卡片信息验证、消息发送模块、卡片退回模块、追访管理模块、报表查询等与服务器通信的相关模块。

(2) 新筛中心综合管理系统

新筛中心综合管理系统在调用通信服务前，应采用对称加密技术对需要传输的业务数据进行加密，加密数据传送至服务器，服务器 web 服务应采用相应解密算法解密业务数据，解密成功后再保存至数据库。子系统的请求数据与服务器的响应数据均需要做加解密处理，保证通信过程中传输的数据均为加密后数据。在传输过程中因数据篡改导致解密异常时，系统自动记录解密异常日志。

所改造内容包括用户登录、卡片扫描验证、卡片数据保存模块、卡片退回模块、门诊接收模块、追访管理模块、复诊管理模块、短信管理模块、电子病历管理模块、报表查询等与服务器通信的相关模块。

(3) 实验室管理系统

实验室管理系统在调用通信服务前，应采用对称加密技术对需要传输的业务数据进行加密，加密数据传送至服务器，服务器 web 服务应采用相应解密算法解密业务数据，解密成功后再保存至数据库。子系统的请求数据与服务器的响应数据均需要做加密解密处理，保证通信过程中传输的数据均为加密后数据。在传输过程中因数据篡改导致解密异常时，系统自动记录解密异常日志。

所改造内容包括用户登录、卡片扫描验证、实验批次管理模块、TSH 实验结果管理模块、PHE 实验结果管理模块、17-OHP 实验结果管理模块、MS/MS 实验结构管理模块、MS/MS 报告管理模块、数据核查模块、报表查询等全部与服务器通信的相关模块。

(4) 中心 web 服务

中心 web 服务在接收到加密的通信数据后，应采用解密算法解密业务数据，再做相应的数据处理，解密失败时应记录数据异常日志，同时系统返回异常信息，通信失败。

所改造内容包括当前 Web 服务中的所有提供对应服务的方法。

(5) 实验室 web 服务

实验室 web 服务在接收到加密的通信数据后，应采用解密算法解密业务数据，再做相应的数据处理，解密失败时应记录数据异常日志，同时系统返回异常信息，通信失败。

所改造内容包括当前 Web 服务中的所有提供对应服务的方法。

6. 项目管理与组织及人员要求

6.1. 项目管理工作内容

在本项目升级改造建设过程中，投标人应在项目管理领域需要完成的工作主要包括：

- (1) 对整体项目进度进行控制，保证项目按时提交。
- (2) 组织协调项目各环节工作，保证项目顺利推进。
- (3) 制定整体项目目标、分阶段目标，并制定各类目标相应的考核计划，规避各类项目风险保证项目质量。
- (4) 管理项目团队的组织和人员，为项目提供组织保障。
- (5) 服从采购人项目组的管理，依从新生儿疾病筛查管理系统整体框架设计和要求，保证新生儿疾病筛查管理系统升级改造工作达到要求。

6.2. 项目管理项目程序和制度要求

投标人应对本项目管理的各环节明确管理实施程序，并制定相关管理制度。

6.3. 项目管理实施方案要求

针对本项目，投标人需提出项目管理的实施方案和措施：

(1) 范围管理措施

投标人应通过需求调研，明确项目的范围，确认工作边界。

(2) 进度控制与过程管理措施

投标人应提出对本项目进度控制和过程的管理措施，对进度控制的过程、进度管理的体系、过程管理方式提供详细方案。

(3) 质量控制措施

投标人应定义本项目的质量控制活动的组织、质量控制任务和质量职责的划分；为执行质量控制任务提供参考资料和指导；为执行质量控制活动提供标准和约定；为质量控制活动和总结提供工具、技术和方法支持。

(4) 风险管理措施

建立风险管理机制，提供风险管理与控制策略，并提供本项目的应急预案。

(5) 档案管理措施

投标人应协助采购人完成项目建设过程中的档案管理工作，明确档案管理职责，采取有效措施对项目后续参建项目形成的档案进行统一管理，保证档案实体和信息的安全。

6.4. 系统管理及文档要求

项目要求中标人交付可执行文件、安装部署文件等，并且知识产权归采购人所有。

项目的工作内容及成果文档的提交应覆盖以下内容，电子文档是成果不可分割的部分。

投标人提供的技术文件与其提供的软件相一致。至少包括：系统需求分析说明书、项目进度计划、系统实施方案、系统测试报告、系统验收报告等。

6.5. 对项目团队人员角色和能力要求

6.5.1. 组织和人员的总体要求

本项目投标人应根据本项目的具体情况，组成由项目管理、系统设计、开发与调试、系统测试、售后等角色构成的项目团队，负责本项目的实施。

本项目投标人应根据本项目的要求，结合本项目的实际特点，从组织结构上满足本项目的要求，合理配置技术支持的人员，选择有丰富经验的人员参与。

(1) 必须成立合理的组织机构，建立健全保障项目顺利实施的各项管理制度和质量保证体系，安排足够的高素质人才参加本项目的建设。

(2) 在项目组织机构中应明确各岗位的职责、任职资格，确保项目顺利实施。应分别配备有业务经验的项目经理、项目技术负责人等人员承担本项目的建设。投标人应承诺项目经理具有 5-10 年相关工作经验，在项目正式验收前专职承担本项目相应工作，合同期内不得更改，正常缴纳社保。

(3) 参与本项目的技术人员应具有 3 年以上相关工作经验，具有强烈的服务意识和高度的责任感。

(4) 采购人不承诺提供开发场地，项目正式启动后，投标人必须保证所有人员能够根据采购人的需要自行解决场地，进行项目集中开发。

6.5.2. 项目团队人员服务要求

(1) 采购人有权对不满足要求的人员要求投标人进行更换；投标人应及时更换相应人员并保证项目进度不受影响；若采购人认为工期和质量无法确保时，投标人须及时增加项目人员。

(2) 投标人承诺提供的项目团队人员服从采购人的工作安排和管理；保证项目团队人员投入本项目的工作时间和任务饱满。项目团队人员应具有吃苦耐劳的工作精神，能按照采购人要求进行加班，由投标人承担由此增加的食宿交通等相关费用。

(3) 投标人成立至少由 3 人组成的项目组，其中 2 名开发和实施人员、至少 1 名测试人员。

6.6. 需求变更要求

项目实施过程中可能产生需求变更，如果需求变更调整在现有基础上的 10% 之内，投标人须承诺视同包含在项目需求之中，不做合同和工期调整。（提供承诺函并加盖投标人公章）。

7. 技术支持与售后服务

投标人应针对系统使用与运行需要，提供详细的售后服务方案及服务承诺书。售后服务方案要从技术支持与服务体系、服务策略、服务组织保障、服务质量保障、服务内容、服务流程、紧急情况响应服务、质保期和用户满意度指标和标准等方面进行详细说明；服务承诺书主要内容包括售后服务响应时间，电话响应时间不大于 10 分钟，2 小时到达现场，4 小时解决问题，暂时无法解决的问题，需告知如何处理。

对此次系统安全升级改造内容应提供两年的免费维护期，免费维护期从项目验收之日起开始计算。

8. 知识产权要求

投标人应承诺本项目实施过程中产生的软件开发成果，相关知识产权、著作权归采购人所有（提供的服务承诺函需加盖投标人公章）。具体要求如下：

（一）采购人对项目实施过程中所产生的所有成果（包括发明及相关代码、技术资料、文档等）享有所有权（永久使用权、复制权和修改权等）。除本项目工作所需外，未经采购人书面同意，投标人不得擅自使用、复制采购人的商标、标志、数据信息、文档及其他资料。

（二）投标人应保证其所提供的产品及服务不侵犯第三方的知识产权，否则，由此给采购人造成的一切损失由投标人承担。

（三）若投标人在本项目中采用第三方软件或产品，投标人需承诺其均为正版。