**北京胸科医院互联互通集成平台测评和咨询服务项目需求说明**

# 项目概述

网络安全等级保护是国家信息安全保障的基本制度、基本策略、基本方法。开展网络安全等级保护工作是保护信息化发展、维护信息安全的根本保障，是信息安全保障工作中国家意志的体现。根据《网络安全法》规定，运营、使用单位或者其主管部门应当按照网络安全等级保护制度的要求，履行网络安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改，并依据《网络安全等级保护基本要求》等技术标准，对信息系统安全等级状况开展等级测评工作。

根据国家卫健委规信司2020年发布的14号文《关于加强全民健康信息标准化体系建设的意见》，意见中提出，要加快全民健康信息平台标准化建设，强化全国医院信息平台标准化建设，执行国家卫健委印发的电子病历数据集、电子病历共享文档等规范、标准，执行《全国医院信息化建设标准与规范(试行)》等文件，加强疾病报告、健康服务等数据的采集与共享，统筹做好电子病历系统应用水平分级评价和卫生健康信息标准应用成熟度评价工作，推进医院信息化标准评价一体化，加快基于电子病历的医院信息平台和临床数据中心建设。

# 项目总体目标

本次第三方测试服务项目的总体工作目标是：完成首都医科大学附属北京胸科医院信息集成平台网络安全等级三级测评，并且对平台互联互通成熟度进行定量咨询服务，以发现其安全保护状况与相应网络安全等级保护要求之间的差距和可能存在的安全隐患，为后续系统安全建设整改和监管机构的监督管理提供参考，同时推进医院信息化标准评价一体化。

# 第三方测试技术规格

## 总体原则

方案设计与项目实施应满足以下原则：

* 公平原则：实施方应遵循“面向应用、保证质量、客观公正、诚信守诺”的原则开展安全评测工作。
* 标准性原则：实施方应依据相关国家标准、行业标准开展评测工作。本评测要求所使用的标准和规范如与实施方所执行的标准不一致时，按较高标准执行。
* 优质服务原则：本评测要求实施方提供的是最低限度的要求，实施方应保证提供符合本评测要求和有关标准的优质服务，并确保评测报告符合项目最终验收的所有要求。
* 保密原则：对评测服务过程中接触到的各种信息，不得泄漏给任何单位和个人，未经允许不得利用这些信息从事与服务无关的活动。

## 项目依据

需遵循的相关标准包括：

* 《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发[2003]27号)
* 《中华人民共和国计算机信息系统安全保护条例》(国务院147号令）
* 《信息安全等级保护管理办法》（公通字[2007]43号）
* 《信息安全等级保护备案实施细则》（公信安[2007]1360号）
* 《计算机信息系统安全保护等级划分准则》（GB 17859—1999）
* 《信息安全技术 网络安全等级保护测评要求》（GB/T 28448—2019）
* 《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449—2018）
* 《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）
* 《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2020）
* WS 445-2014（所有部分）电子病历基本数据集
* WS/T 447-2014 基于电子病历的医院信息平台技术规范
* GB/T 14396-2016 疾病分类与代码
* WS/T 482-2016 卫生信息共享文档编制规范
* WS/T 500-2016（所有部分）电子病历共享文档规范
* T/CHIA 001-2017 手术、操作分类与代码
* 医院信息平台基本交互规范

## 项目需求

## 网络安全等级保护测评要求

### 信息系统差距分析服务

信息系统安全等级保护差距分析将根据《信息安全技术网络安全等级保护测评要求》、《信息安全技术网络安全等级保护测评过程指南》等标准文件的要求，对已定级信息系统，进行系统现状调研，逐项进行合规性检测。其实质是采用基线安全分析的方法，明确当前信息系统与等级保护要求的不符合项及差距。依据信息系统定级情况，对信息系统的各项安全指标进行符合性评估，标识信息系统的不符合项，明确信息系统与等级保护基本要求之间的差距。

* 根据项目的总体要求及信息系统等级保护体系建设现状需要，对信息系统进行差距分析，从安全技术差距分析测评和安全管理差距分析测评两部分进行，对系统各项安全指标进行符合性评估，并标识系统不符合项，明确系统与国家安全等级保护相关标准要求的差距。
* **交付成果**

《信息系统差距分析报告》

### 信息系统整改咨询服务

信息系统安全建设整改咨询主要是依据差距分析报告，对被测信息系统面临的安全风险进行总结分析，对信息系统不符合信息系统等级保护建设基本要求的部分提供可行性整改建议或方案，从整体上把控内容，主要从技术和管理两方面进行整改，最终能够使被测信息系统在进行安全建设整改后可通过等级保护测评。

* **交付成果**

《信息系统安全整改建议书》

### 信息系统等级保护测评服务

依据GB/T 28448-2019《信息安全技术网络安全等级保护测评要求》、GB/T22239-2019《信息安全技术网络安全等级保护基本要求》对项目进行正式的信息安全等级保护测评及复测评，出具公安部门认可的网络安全等级测评报告。信息系统安全等级测评主要检测和评估信息系统在安全技术、安全管理等方面是否符合已确定的安全等级三级的要求，对于尚未符合要求的信息系统，分析和评估其潜在威胁、薄弱环节以及现有安全防护措施，综合考虑信息系统的重要性和面临的安全威胁等因素，提出相应的整改建议，最终用户根据初次等级保护测评工作中发现的问题进行整改，待整改工作结束后，进行等级保护复测确认，以确保信息系统的安全保护措施符合相应安全等级三级的基本要求，并提交符合国家等级保护测评三级要求的等级保护测评报告。

* **交付成果**

《网络安全等级保护测评报告》**（测评完成后提交加盖检测专用章并符合公安部门安全等级保护要求的测评报告）**

## 定量咨询服务

在互联互通改造阶段需要提供标准化自测服务如下：

一、提供定量标准化改造自测咨询服务，包括定量测评相关技术问题解答；

二、两次模拟测试：在搭建好环境，准备好相关标准要求的xml文档后，进行2次在线模拟测试；

三、对现场查验定量部分需要准备的工作和资料、注意事项进行培训。

# 项目管理及服务要求

## 服务保证

应严格执行项目管理规定，从项目组织管理、项目进度管理、项目质量保障和安全保密等方面加强项目管理，确保服务质量。

## 质量保证

应建立严格的质量保证体系，制定项目建设的质量控制方案和实施措施，并督促落实各环节质量控制内容和目标；保证项目各个阶段工作满足招标方对质量的要求。

## 工期保证

（1）在本项目合同签订之后，按合同约定完成相关工作。

（2）项目进度管理应该遵循以下原则：

* 项目进度管理的依据是项目合同所约定的工期目标；
* 在确保项目质量和安全的原则下，控制项目进度。

（3）项目进度管理应该至少包含以下内容：

* 在了解项目详细情况后，按照合同约定工期制定具体实施计划，明

确各阶段工作任务；

* 按照具体实施计划，定期跟踪检查，对可能发生的延误提出相应对

策。