XXXXXXX
XXXX

WS

中 华 人 民 共 和 国 卫 生 行 业 标 准

WS XXX—201X

# 电子健康卡技术规范 第6部分：联网检测

**Technical specification for electronic health card Part 6：**

**Networking testing**

（征求意见稿）

201X-XX-XX 发布　　201X-XX-XX 实施

国家卫生健康委员会 发布

# 目　次

1 范围 ..... 1
2 规范性引用文件 ..... 1
3 术语和定义 ..... 1
3.1 电子健康卡 ..... 1
3.2 电子健康卡管理系统 ..... 1
3.3 主索引 ID ..... 1
3.4 电子健康卡 ID ..... 1
3.5 电子健康卡二维码 ..... 2
3.6 密码设备 ..... 2
3.7 接入机构 ..... 2
3.8 接入 APP ..... 2
3.9 识读终端 ..... 2
4 检测概述 ..... 2
5 技术要求检测 ..... 3
5.1 安全检测 ..... 3
5.1.1 系统安全 ..... 3
5.1.2 网络安全 ..... 5
5.1.3 主机安全 ..... 7
5.1.4 物理安全 ..... 8
5.2 功能检测 ..... 8
5.3 性能效率检测 ..... 10
5.4 接口检测 ..... 11
5.5 系统灾备 ..... 11
6 管理要求核查 ..... 12
6.1 管理机构 ..... 12
6.2 管理制度 ..... 13
6.3 人员管理 ..... 13
6.4 建设管理 ..... 14
6.5 运维管理 ..... 15
7 结果判定准则 ..... 16
7.1 必选项 ..... 16
7.2 推荐项 ..... 16

# 前　言

本标准由卫生部卫生信息标准专业委员会提出。

本标准主要起草单位：国家卫生健康委员会。

本标准主要起草人：

# 电子健康卡技术规范 第6部分：联网检测

## 1 范围

本规范规定了电子健康卡管理系统现场综合检测的检测过程、检测方法、检测内容和检测结果判定准则等。

本规范适用于三方面的检测：

——电子健康卡管理系统联网的安全检测；

——电子健康卡管理系统联网的接口检测；

## 2 规范性引用文件

下列文件对于本规范的应用是必不可少的。凡是注日期的引用文件，其随后所有的修改单(不包括刊物的内容)或修订版均不适用于本规范，然而，鼓励根据本规范达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本规范。

GB/T 9386-2008 计算机软件检测文档编制规范；

GB/T 20158-2006 信息技术软件生存周期过程配置管理；

GB/T 25000.51-2016 系统与软件工程 系统与软件质量要求和评价（SQuaRE） 第 51 部分：就绪可用软件产品（RUSP）的质量要求和检测细则；

GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求；

居民健康卡虚拟化应用建设指导方案（试用）V1.7。

## 3 术语和定义

下列术语和定义适用于本规范。

### 3.1 电子健康卡

通过用户身份标识建立的电子健康卡虚拟化账户，电子健康卡虚拟化账户使用时，可通过二维码形式展现为电子健康卡，功能与实体居民健康卡相同。

### 3.2 电子健康卡管理系统

在电子健康卡注册用卡过程中，负责电子健康卡发卡数据的生产、使用和管理，采用电子账户对信息进行存储，并支持线下交互的技术应用。

### 3.3 主索引 ID

是标识居民健康卡用户唯一性的信息，通过主索引 ID 关联用户的实体居民健康卡、电子健康卡、医院就诊卡等不同类型账户。

### 3.4 电子健康卡 ID

电子健康卡管理系统用于标识电子健康卡账户唯一性的信息，电子健康卡 ID 由用户的证件类型和证件号码的密文组成。

### 3.5 电子健康卡二维码

电子健康卡通过二维码的形式予以展示，通过“面对面”方式进行交互使用。电子健康卡二维码包括静态二维码和动态二维码：静态二维码可通过移动APP呈现，也可印刷或粘贴于就诊卡等介质上，适用于挂号、问诊等非核心应用场景；动态二维码由APP呈现，在每次使用前生成，其生命周期根据应用安全的要求限定时间范围，适用于病历查询、结算交易等核心应用场景。

### 3.6 密码设备

密码设备是具有某种密码功能或能完成某种密码工作任务的设备的统称。

### 3.7 接入机构

接入使用居民健康卡虚拟化平台，与平台提供接口存在交互逻辑的相关机构事业单位，包括但不限于医疗卫生机构、医保机构等。

### 3.8 接入 APP

接入居民健康卡虚拟化应用平台，与平台接口存在交互逻辑的互联网移动应用。

### 3.9 识读终端

识读二维码并与后台应用系统进行交互的终端，一般包括二维码的识读设备和终端机上的应用软件。

## 4 检测概述

通过在实验室的检测和深入理解，对系统检测需求进一步解读,联网检测需在现场对系统的核心业务功能、安全、性能指标进行科学的检测设计和有效地评测组织实施。检测机构独立、客观、公正、定量地分析评估和报告被测系统的整体状况，提交系统存在的缺陷，提出系统的改进建议，通过整改验证使系统达到一个稳定可靠的质量状态。

联网检测总体目标如下：

- 功能性

系统在实验室检测通过后在现场验证运行是否正常，确保实际业务使用的需求流程和功能均被实现，且没有在检测和使用过程没有中断的情况发生。

- 可靠性

系统是否满足了实际业务需求中对系统可靠性的要求，系统可以有效的控制业务交叉，保障系统可以在遇到大数据量或软件故障的同时具有较强的失效防护能力，并保障数据精度及业务一致性的能够达到实际业务中的真实需求。

➢ 安全性

**联网检测前或在承诺的时间内通过信息安全等级保护二级以上（含二级）测评，并在联网检测中对信息安全技术的管理安全和技术安全核心指标验证，**确保系统具有防止对程序或数据或信息被非授权访问的能力，系统中不存在各种具有安全隐患的漏洞及不必要的开放端口，整体安全架构符合实际业务系统对安全性的要求。

➢ 性能效率

核实系统的业务在所指定的事务或业务功能在正常的预期工作量、预期峰值工作量下的的处理时间及资源利用率能够满足实际业务需求，并且系统需具备7*24小时不间断稳定运行的能力。

## 5 技术要求检测

### 5.1 安全检测

#### 5.1.1 系统安全

| 序号 | 检测项 | 检测内容 | 检测方法及步骤 | 预期结果及判定 | 检测要求 |
|---|---|---|---|---|---|
| 1. | 系统扫描 | 电子健康卡管理系统进行安全漏洞扫描检测，未存在高、中级别安全风险。 | 使用软件工具或测试工具箱进行扫描测试。 | 系统未存在高、中级别安全风险。 | 必选项 |
| 2. | 访问控制 | 电子健康卡管理系统的应用服务器和数据库服务器位于内部网络区域，与互联网之间有 DMZ 区隔离。 | 检查网络拓扑图和数据环境。 | 系统与互联网之间隔离。 | 必选项 |
| 3. | | 电子健康卡管理系统的管理人员终端专属运维终端，与互联网进行隔离。 | 访谈管理人员并检查管理终端。 | 管理终端与互联网之间隔离。 | 必选项 |

| 序号 | 检测项 | 检测内容 | 检测方法及步骤 | 预期结果及判定 | 检测要求 |
|---|---|---|---|---|---|
| 4. | | 电子健康卡管理系统的管理人员拥有独立的账户，非管理人员未授权不能访问。 | 访谈管理人员并检查账户使用情况。 | 管理员独立帐号，非管理员未授权不能访问。 | 必选项 |
| 5. | | 系统的管理人员终端安装了防病毒软件。 | 访谈管理人员并检查管理终端。 | 管理人员终端安装了防病毒软件。 | 必选项 |
| 6. | 通信安全 | 电子健康卡管理系统对互联网、专网提供的服务（手机客户端、微信等），通信应是安全的。（通讯安全手段如加密协议、ipsec vpn 等手段）。 | 现场检查并评审电子健康卡管理系统对互联网提供的通信是否安全。 | 电子健康卡管理系统对互联网提供通信是安全的 | 必选项 |
| 7. | | APP 终端/微信公众号/支付宝服务号的后台服务器通信应是安全的。（通讯安全手段如加密协议、ipsec vpn 等手段）。 | APP 终端/微信公众号/支付宝服务号的后台服务器提供的通信是否安全。 | APP 终端/微信公众号/支付宝服务号的后台服务器通信是安全的 | 必选项 |
| 8. | 系统防护 | 系统防护策略包括：<br>删除或者禁用不使用的账户；<br>限制密码长度（推荐 8 位及以上）；<br>设置密码复杂度（包含字母和大小写数字）；<br>限制密码使用期限（90 天强制修改密码）； | 检查并测试验证系统对账户的安全管理机制。 | 删除或者禁用不使用的账户；<br>限制密码长度 8 位及以上；<br>设置密码复杂度包含字母和大小写数字；<br>限制密码使用 90 天强制修改密码；<br>设置访问空闲超时 10 分钟；<br>默认管理员账户未授权不能远程 | 必选项 |

| 序号 | 检测项 | 检测内容 | 检测方法及步骤 | 预期结果及判定 | 检测要求 |
|---|---|---|---|---|---|
| | | 设置访问空闲超时（推荐 10 分钟）；默认管理员账户未授权不能远程登录设备。 | | 登录设备。 | |

### 5.1.2 网络安全

网络安全检测包括电子卡管理系统所在环境中的所关联的网络设备，互联网检测前需调研统计分析需要检测网络设备清单。

网络安全的可选择需要提供安全保障/承诺书。

| 序号 | 检测项 | 检测内容 | 检测方法及步骤 | 预期结果及判定 | 检测要求 |
|---|---|---|---|---|---|
| 1. | 网络扫描 | 对网络设备进行安全漏洞扫描检测，未存在高、中级别安全风险。 | 使用软件工具或测试工具箱进行扫描测试。 | 网络设备未存在高、中级别安全风险。 | 必选项 |
| 2. | 结构安全 | 绘制与当前运行情况相符的网络拓扑结构图。 | 检查网络拓扑图和实际网络环境是否一致 | 拓扑图和实际网络环境一致。 | 可选项 |
| 3. | | 根据各部门的工作职能、重要性、所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段。 | 检查并网段分配和区域划分 | 根据实际情况合理划分不同的子网或网段。 | 可选项 |
| 4. | | 重要网段应采取网络层地址与数据链路层地址绑定措施，防止地址欺骗。 | 检查安全设备绑定配置，并验证配置 | 重要网段采取网络层地址与数据链路层地址绑定。 | 可选项 |
| 5. | 访问控制 | 能根据会话状态信息为数据流提供明确的允许/拒绝访 | 检测网络设备对用户访问权限的控制 | 可对访问用户进行允许/拒绝访问的能力，控制粒度为端口级。 | 可选项 |

| 序号 | 检测项 | 检测内容 | 检测方法及步骤 | 预期结果及判定 | 检测要求 |
|---|---|---|---|---|---|
| | | 问的能力，控制粒度为端口级。 | | | |
| 6. | | 会话处于非活跃一定时间或会话结束后终止网络连接。 | 检测网络设备对用户访问权限的控制 | 访问用户会话结束后终止网络连接 | 可选项 |
| 7. | | 限制网络最大流量数及网络连接数。 | 检测网络设备对用户访问权限的控制 | 可对访问用户进行流量和连接数控制。 | 可选项 |
| 8. | 安全审计 | 对网络系统中的网络设备运行状况、网络流量、用户行为等进行全面的监测、记录。 | 检查网络设备是否有安全审计功能 | 网络设备有安全审计功能。 | 可选项 |
| 9. | | 可以根据记录数据进行分析，并生成审计报表。 | 检查记录的数据是否可以到处报表 | 记录数据生成审计报表。 | 可选项 |
| 10. | 入侵防范 | 在互联网边界区域部署防火墙等安全设备进行防护，防护的策略是有效的。 | 1、检查网络边界防火墙。<br>2、使用工具测试验证防火墙策略是否有效。 | 网络边界区部署了防火墙设备，防火墙安全策略有效。 | 可选项 |
| 11. | | 在关键网络节点部署 IPS/IDS 等入侵防范设备进行入侵防范，防护的策略是有效的。 | 1、检查关键网络节点是否部署 IPS/IDS 设备。<br>2、使用工具测试验证入侵防反策略是否有效。 | 关键网络节点部署入侵防范设备进行入侵防范，防护的策略是有效的。 | 可选项 |
| 12. | | 在关键网络节点部署防 DDoS 攻击的设备，防护的策略是有效的。 | 1、检查关键网络节点是否部署 DDOS 设备。<br>2、使用工具测试验证入侵防反策略是否有效。 | 关键网络节点部署防 DDoS 攻击的设备，防护的策略是有效的。 | 可选项 |
| 13. | 设备防护 | 网络设备防护策略包括：<br>删除或者禁用不使用的系统缺省账 | 检查并测试验证系统对账户的安全管理机制。 | 删除或者禁用不使用的账户；<br>限制密码长度 8 位及以上；<br>设置密码复杂度 | 必选项 |

| 序号 | 检测项 | 检测内容 | 检测方法及步骤 | 预期结果及判定 | 检测要求 |
|---|---|---|---|---|---|
| | | 户；<br>限制密码长度（推荐 8 位及以上）；<br>设置密码复杂度（包含字母和大小写数字）；<br>限制密码使用期限（90 天强制修改密码）；<br>设置访问空闲超时（推荐 10 分钟）；<br>默认管理员账户未授权不能远程登录设备。 | | 包含字母和大小写数字；<br>限制密码使用 90 天强制修改密码；<br>设置访问空闲超时 10 分钟；<br>默认管理员账户未授权不能远程登录设备。 | |

### 5.1.3 主机安全

主机安全检测包括电子卡管理系统所在环境中的所关联的应用服务器、数据库服务器、存储服务器关联的设备，互联网检测前需调研统计分析需要检测的主机设备清单。

| 序号 | 检测项 | 检测内容 | 检测方法及步骤 | 预期结果及判定 | 检测要求 |
|---|---|---|---|---|---|
| 1. | 主机扫描 | 对主机系统进行安全漏洞扫描检测，未存在高、中级别安全风险。 | 使用软件工具或测试工具箱进行扫描测试。 | 主机系统未存在高、中级别安全风险。 | 必选项 |
| 2. | 主机防护 | 主机防护策略包括：<br>删除或者禁用不使用的系统缺省账户；<br>限制密码长度（推荐 8 位及以上）；<br>设置密码复杂度（包含字母和大小写数字）； | 检查并测试验证系统对账户的安全管理机制。 | 删除或者禁用不使用的账户；<br>限制密码长度 8 位及以上；<br>设置密码复杂度包含字母和大小写数字；<br>限制密码使用 90 天强制修改密码；<br>设置访问空闲超时 10 分钟； | 必选项 |

| 序号 | 检测项 | 检测内容 | 检测方法及步骤 | 预期结果及判定 | 检测要求 |
|---|---|---|---|---|---|
| | | 限制密码使用期限（90 天强制修改密码）；<br>设置访问空闲超时（推荐 10 分钟）；<br>默认管理员账户未授权不能远程登录设备。 | | 默认管理员账户未授权不能远程登录设备。 | |
| 3. | 病毒防范 | 服务器和终端设备（包括移动设备）均应安装实时检测和查杀病毒的软件产品。 | 检查主机服务器是否安装了查杀病毒的软件产品 | 服务器和终端设备均应安装实时检测和查杀病毒的软件产品。 | 必选项 |

5.1.4　物理安全

| 序号 | 检测项 | 检测内容 | 检测方法及步骤 | 预期结果及判定 | 检测要求 |
|---|---|---|---|---|---|
| 1. | 物理位置 | 电子健康卡管理系统和加密机的位置与应用服务器处于同一区域。 | 检查电子健康卡管理系统和加密机的位置 | 电子健康卡管理系统和加密机同一区域。 | 必选项 |
| 2. | | 机房应选择在具有防震、防风和防雨等能力的建筑内。 | 检查机房场所 | 机房具有防震、防风和防雨等能力的建筑内。 | 必选项 |
| 3. | 防破坏 | 通信线缆铺设在隐蔽处，如铺设在地下或管道中等。 | 检查机房场所 | 通信线缆铺设在隐蔽处。 | 必选项 |
| 4. | 访问控制 | 对重要区域配置电子门禁系统，鉴别和记录进入的人员身份并监控其活动。 | 检查机房场所 | 对重要区域配置电子门禁系统。 | 必选项 |

5.2　功能检测

| 序号 | 检测对象 | 检测项 | 检测内容 | 检测方法及步骤 | 预期结果及判定 | 检测要求 |
|---|---|---|---|---|---|---|
| 1. | 电子健康卡管理系统 | 系统版本 | 系统已经在实验室通过检测的，系统应是送检实验室版本或高于实验室版本（版本更新应有版本更新记录说明）。 | 查看系统版本 | 系统是送检实验室版本或高于实验室版本。 | 必选项 |
| 2. | | 用户管理 | 系统自身具有用户管理以及用户权限管理功能。 | 检查系统管理权限 | 具有用户权限管理功能。 | 必选项 |
| 3. | 密码机 | 接入许可 | 密码机是通过检测的型号，电子健康卡管理系统的密码机 dll 与检测版本一致。 | 检查密码机型号和版本 | 通过检测的型号，密码机 dll 与检测版本一致。 | 必选项 |
| 4. | | 密码机验证 | 电子健康卡管理系统已对接密码机，断开密码机业务不能正常使用。 | 断开密码机验证 | 电子电子健康系统业务依赖于密码机。 | 必选项 |
| 5. | 识度终端 | 接入许可 | 识度终端是通过检测的型号。 | 检查识度终端版本 | 识度终端是通过检测的型号。 | 必选项 |
| 6. | 客户端应用 APP/微信公众号/支付宝服务号 | 接入许可 | APP、微信公众号、支付宝服务号应该具有客户端应用软件接入检测报告。 | 检查互联网网终端是否有接入检测报告 | 互联网网终端是有接入检测报告。 | 必选项 |
| 7. | 全流程验证 | 全流程展示验证 | 应用场景对关键业务（医院就诊全流程）验证。**包括；医院窗口二维码领取流程和医院自助终端** | 在医院模拟就诊全流程 | 医院可实现二维码全流程就诊。 | 必选项 |

| 序号 | 检测对象 | 检测项 | 检测内容 | 检测方法及步骤 | 预期结果及判定 | 检测要求 |
|---|---|---|---|---|---|---|
| | | | 流程。 | | | |

## 5.3 性能效率检测

性能效率的可选择需要提供安全保障/承诺书。

| 序号 | 检测对象 | 检测项 | 检测内容 | 检测方法及步骤 | 预期结果及判定 | 检测要求 |
|---|---|---|---|---|---|---|
| 1. | 电子健康卡管理系统 | 用户注册 | 用户注册多用户并发成功率100%；单笔交易响应时间不超过 1s 。（检测建议指标：在30个用户并发时，TPS（Transactions per second）应不低于30。） | 使用软件工具或测试工具箱开发脚本模拟真实用户访问场景进行并发测试 | 在30个用户并发时，TPS（Transactions per second）应不低于30。 | 必选项 |
| 2. | | 二维码生成 | 二维码生成多用户并发成功率100%；单笔交易响应时间不超过 1 秒。（检测建议指标：在30 个用户并发时，TPS（Transactions per second）应不低于30。） | 使用软件工具或测试工具箱开发脚本模拟真实用户访问场景进行并发测试 | 在30个用户并发时，TPS（Transactions per second）应不低于30。 | 必选项 |
| 3. | | 二维码验证 | 二维码验证多用户并发成功率 100%；单笔交易响应时间不超过 1 秒。（检测建议指标：在30 个用户并发时，TPS | 使用软件工具或测试工具箱开发脚本模拟真实用户访问场景进行并发测试。 | 在30个用户并发时，TPS（Transactions per second）应不低于30。 | 必选项 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | （Transactions per second）应不低于30。） | | | |
| 4. | 网络性能 | 互联网出口带宽 | 出口带宽应满足系统预期设计用户数的访问要求，带宽大于20Mbps | 使用软件工具或测试工具箱对出口带宽测试。 | 带宽大于20Mbps。 | 可选项 |
| 5. | | 医疗机构专网带宽 | 医疗机构专网带宽应满足系统预期设计用户数的访问要求，带宽大于50Mbps | 使用软件工具或测试工具箱对专网带宽测试。 | 带宽大于50Mbps。 | 可选项 |
| 6. | 稳定性检测 | 不间断稳定运行 | 系统整体具备7*24小时不间断稳定运行。 | 使用软件工具或测试工具箱开发脚本模拟真实用户访问场景进行长时间测试。 | 7*24小时不间断稳定运行。 | 推荐项 |

## 5.4 接口检测

| 序号 | 检测项 | 检测内容 | 要求 |
|---|---|---|---|
| 1. | 支付接口（如有） | 支付业务接口正常使用。 | 必选项 |
| 2. | 识度终端接口 | 识度业务接口正常使用。 | 必选项 |
| 3. | APP接口/微信公众号/支付宝服务号 | APP接口/微信公众号/支付宝服务接口正常使用。 | 必选项 |
| 4. | 机构连接接口 | 结构业务接口正常使用。 | 必选项 |
| 5. | 密码机接口 | 密码机接口可正常使用。 | 必选项 |
| 6. | 用户注册 | 用户注册接口可正常使用。 | 必选项 |
| 7. | 二维码生成 | 二维码生成接口可正常使用。 | 必选项 |
| 8. | 二维码验证 | 二维码验证接口可正常使用。 | 必选项 |
| 9. | 监测平台接口 | 监测平台业务接口可正常使用。 | 必选项 |
| 10. | 国家平台接口 | 国家平台业务接口可正常使用。 | 必选项 |

## 5.5 系统灾备

性能效率的可选择需要提供安全保障/承诺书。

| 序号 | 检测项 | 检测内容 | 要求 |
|---|---|---|---|
| 1. | 电子健康卡管理系统 | 电子健康卡管理系统应用服务器具有双机热备机制，并验证双机热备机制有效。 | 必选项 |
| 2. | | 电子健康卡管理系统数据库服务器具有双机热备机制，并验证双机热备机制有效。 | 必选项 |
| 3. | | 电子健康卡管理系统和数据具有备份和恢复策略，对关键数据定期备份，备份数据应保密并有专人管理。 | 必选项 |
| 4. | 网络设备 | 防火墙设备具有双机热备机制，并验证双机热备机制有效。 | 可选项 |
| 5. | | 交换机设备具有双机热备机制，并验证双机热备机制有效。 | 可选项 |
| 6. | 密码机 | 密码机设备具有双机热备机制，并验证双机热备机制有效。 | 可选项 |
| 7. | 其他网络设备 | IDS、IPS、网闸、DDOS 设备具有双机热备机制，并验证双机热备机制有效。 | 可选项 |

## 6 管理要求核查

### 6.1 管理机构

| 序号 | 检测项 | 检测内容 | 检测方法及步骤 | 预期结果及判定 | 检测要求 |
|---|---|---|---|---|---|
| 1. | 人员配备 | 设立系统管理人员、网络管理人员、安全管理人员岗位，定义各个工作岗位的职责。 | 访谈管理人员并检查管理要求 | 定义各个工作岗位的职责。 | 必选项 |
| 2. | | 建立各审批事项的审批程序，按照审批程序执行审批过程。 | | 按照审批程序执行审批过程。 | 推荐项 |
| 3. | | 专职安全管理人员不可兼任。 | | 安全管理人员专职。 | 必选项 |
| 4. | 审核检查 | 安全管理人员定期进行安全检查，检查内容包括用户账 | | 定期进行安全检查。 | 必选项 |

| | | | | | |
|---|---|---|---|---|---|
| | | 号情况、系统漏洞情况、系统审计情况。 | | | |
| 5. | 沟通机制 | 与供应商、业界专家、专业的安全公司、安全组织的合作与沟通机制。 | | 对外建立安全沟通机制。 | 推荐项 |

6.2 管理制度

| 序号 | 检测项 | 检测内容 | 检测方法及步骤 | 预期结果及判定 | 检测要求 |
|---|---|---|---|---|---|
| 1. | 管理制度 | 安全管理活动中的各类管理内容建立安全管理制度，以规范安全管理活动，约束人员的行为方式。 | 访谈管理人员并检查管理要求 | 建立安全管理制度。 | 必选项 |
| 2. | 审核修订 | 对安全管理制度进行评审和修订，对存在不足或需要改进的安全管理制度进行修订。 | | 安全管理制度进行评审和修订过程。 | 必选项 |

6.3 人员管理

| 序号 | 检测项 | 检测内容 | 检测方法及步骤 | 预期结果及判定 | 检测要求 |
|---|---|---|---|---|---|
| 1. | 人员管理 | 对管理人员、安全管理人员应签署保密协议。 | 访谈管理人员并检查管理要求 | 管理人员、安全管理人员签署保密协议。 | 必选项 |
| 2. | 安全培训 | 制定安全教育和培训计划，对信息安全基础知识、岗位操作规程等进行培训。 | | 制定安全教育和培训计划。 | 必选项 |
| 3. | 第三方访问管理 | 第三方人员应在访问或接入系统前与机构签署安全责任 | | 第三方人员应在访问管理制度。 | 必选项 |

| | | | | | |
|---|---|---|---|---|---|
| | | 合同书或保密协议。 | | | |
| 4. | | 重要区域的访问，须提出书面申请，批准后由专人全程陪同或监督，并记录备案。 | | 重要区域的访问管理。 | 必选项 |

## 6.4 建设管理

| 序号 | 检测项 | 检测内容 | 检测方法及步骤 | 预期结果及判定 | 检测要求 |
|---|---|---|---|---|---|
| 1. | 建设管理 | 开发环境与实际运行环境物理分开。 | 检查系统环境 | 开发环境与实际运行分开。 | 必选项 |
| 2. | | 应指定或授权专门的部门负责系统检测验收的管理，并按照管理制度的要求完成系统检测验收工作。 | 检查验收工作 | 指定或授权专门的部门负责系统检测验收的管理。 | 推荐项 |
| 3. | | 系统属性等资料报系统主管部门备案。 | 检查报备情况 | 在国家卫计委具有备案。 | 必选项 |
| 4. | | 在应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动预案的条件、应急处理流程、系统恢复流程和事后教育和培训等内容。 | 访谈管理人员并检查应急预案 | 制定不同事件的应急预案。 | 必选项 |
| 5. | | 对供应商进行有效管理，约定供应商（硬件和软件服务商）的 SLA。 | 访谈管理人员并检查供应商管理制度 | 供应商进行有效管理。 | 推荐项 |
| 6. | | 定期安全评估；提供等级保护三级报 | 检查是否定期做安全评估，并且等级保护三级报 | 定期做安全评估，提供等级保护三级报告和等 | 必选项 |

| | | | | | |
|---|---|---|---|---|---|
| | | 告，报告必须包含电子健康卡应用系统涉及的机房和网络设备的范围。<br>并应提供年度等级保护计划，要求对电子健康卡系统进行三级评估。 | 告 | 保年度计划。 | |

6.5 运维管理

| 序号 | 检测项 | 检测内容 | 检测方法及步骤 | 预期结果及判定 | 检测要求 |
|---|---|---|---|---|---|
| 1. | 运维管理 | 电子健康卡管理系统的管理和运维进行了培训，并有培训记录。 | 访谈管理人员并检查运维管理制度 | 运维进行了培训，并有培训记录。 | 推荐项 |
| 2. | | 运维人员操作终端是专属运维终端，与互联网进行隔离的。 | | 操作终端是专属运维终端。 | 推荐项 |
| 3. | | 运维人员终端安装了防病毒软件。 | | 运维人员终端安装了防病毒软件。 | 推荐项 |
| 4. | | 运维人员拥有独立的账户，并总是使用自己的账户。 | | 运维人员拥有独立的账户。 | 推荐项 |
| 5. | | 制定系统安全管理制度，对系统安全配置、系统帐户以及审计日志等方面作出规定。 | | 定系统安全管理制度。 | 推荐项 |
| 6. | | 专人对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作。 | | 专人对网络进行管理。 | 推荐项 |

| | | | | | |
|---|---|---|---|---|---|
| 7. | | 定期进行网络系统漏洞扫描，对发现的网络系统安全漏洞进行及时的修补。 | | 对发现的网络系统安全漏洞进行及时的修补。 | 推荐项 |
| 8. | | 规定备份信息的备份方式（如增量备份或全备份等）、备份频度（如每日或每周等）、存储介质、保存期等。 | | 规定备份信息的备份方式。 | 推荐项 |

## 7 结果判定准则

### 7.1 必选项

在技术要求检测、管理要求核查中要求为“必选项”的，在联网检测中要求必须通过，如未通过要求整改，整改后重新验证。

### 7.2 推荐项

在技术要求检测、管理要求核查中要求为“推荐项”的，在联网检测中未要求必须通过，建议整改。