电子健康卡系统平台安全运行技术要求

（V1.0）

国家卫生健康委统计信息中心

2022 年 10 月

目　录

引　言

电子健康卡是国家卫生健康委员会制定统一标准并推广的居民就医和健康服务统一介质，旨在为全体居民建立个人健康的统一身份，解决“一院一卡、多卡并存、互不通用”就医堵点问题，建立“互联网+医疗”便民服务与全生命周期健康管理的统一服务入口。电子健康卡系统平台是各类医疗卫生机构信息互认共享的重要基础平台，是保障城乡居民实施自我健康管理的重要基础工具，是全民健康保障工程的重要基础设施。

电子健康卡系统平台的安全稳定运行对于方便群众就医和个人健康管理具有重要意义。尤其在疫情防控期间，公众对该平台的依赖日益增强，平台面临的安全防护压力加大，网络安全风险不断加剧与防护能力整体不足的矛盾日益凸显。“十四五”是电子健康卡系统平台升级改造和安全运行的成长期、攻坚期、突破期，平台的建设单位应持续增强风险意识、底线思维、安全意识，贯彻落实《中华人民共和国网络安全法》《中华人民共和国密码法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等国家相关法律法规要求。建设单位应结合自身基础和特点，根据有关要求，加强平台的保护管理要求、技术措施落实，加强安全保护机制、能力建设。坚持问题导向，聚焦应对境外高级持续性威胁（APT）、网络勒索、数据窃取等风险威胁，突出平台数据的全生命周期安全管理和平台的供应链安全保障，不断夯实主动防护、监测预警、应急响应、快速恢复能力，及时发现重大安全隐患、修补高危漏洞，以实战化、体系化、常态化为理念，推进动态防御、主动防御、纵深防御、精准防护、整体防护、联防联控，全面保障平台业务运行安全、数据安全、供应链安全，逐步形成全方位、多层次的综合保护屏障。

根据各电子健康卡建设单位对系统信息安全和运行可靠性等方面的需求，国家卫生健康委统计信息中心组织相关省市卫生健康委及专业机构专家，联合研究编制了本技术要求，用于指导各建设单位规范开展电子健康卡系统平台安全建设及运行维护工作。主要内容包括总体要求、电子健康卡系统平台安全架构、安全技术要求、可靠运行要求、部署要求、安全管理要求等。

牵头起草单位：国家卫生健康委统计信息中心

主要参研单位：辽宁省卫生健康服务中心信息化推进办公室、山东省卫生健康委医疗服务中心、湖南省卫生健康委信息统计中心、四川省卫生健康委信息中心、厦门市健康医疗大数据中心、广州市卫生健康技术鉴定和人才评价中心、武汉市卫生健康信息中心、北京市西城区智慧健康研究中心、中国软件评测中心（工业和信息化部软件与集成电路促进中心）、中国关键信息基础设施技术创新联盟、国家信息技术安全研究中心。

电子健康卡系统平台安全运行技术要求

一、总体要求

（一）提升平台的安全管理能力

根据相关法律法规和规章制度要求，按照谁主管谁负责、谁运营谁负责原则，电子健康卡系统平台各建设单位应进一步深化各方职责落实，分工合作，共同做好平台安全保护工作。

加强主体责任落实。各建设单位应加强主体责任落实，按照有关法律法规要求，建立安全保护工作责任机制，加强安全管理责任人、关键岗位及人员责任落实，强化履行安全保护工作职责，完善责任制和考核评价制度。

加强平台建设安全运维保障管理。各建设单位应建立配套制度落实，针对运维保障机构，重点明确系统数据等方面的管理要求；针对网络安全服务机构，重点提出安全建设、日常运维、技术检测、安全监测、应急处置等方面的安全管理要求，严格管理平台建设运行及其安全数据，防止数据泄露。

建立健全移动互联网应用的安全风险动态监测管理机制。加强移动应用资产管理、安全风险管理和个人信息保护管理，对发现的漏洞和潜在的风险及时采取补救措施，对于仿冒、钓鱼类应用的出现及时通知应用渠道管理方进行下架处理。落实网络安全主体责任，应对电子健康码客户端应用软件安全运行情况实时掌控，以满足网络安全部门在移动应用安全方面的政策性和合规性要求。

（二）提升安全防护与运营水平

电子健康卡系统平台各建设单位应按照法律法规、部门规章、规范性文件的规定以及国家标准的强制要求，结合单位实际，对平台采取技术措施和其他必要措施加强防护。

对于与电子健康卡系统平台存在数据交互的互联网、业务网、生产网等，各建设单位应强化网络的合理划分和边界防护，强化商用密码应用，确保互联网安全接入、终端设备有效管控、重要数据和个人信息不被泄露、窃取、篡改等。

各建设单位应定期对平台开展网络安全等级保护（以下简称“等保”）测评及商用密码应用安全性评估（以下简称“密评”）。重点检测卡管系统、跨域主索引系统等关键系统、客户端应用软件和服务器设备的安全性及可能存在的漏洞后门情况。对相关测评过程中发现的问题及时整改加固。

（三）强化数据安全管理和个人信息保护

电子健康卡系统平台各建设单位应从分类分级保护、跨域传输管理、安全评估等多个方面逐步强化数据安全管理和个人信息保护。

加强数据容灾备份。各建设单位应重点针对平台掌握的重要数据、敏感个人信息和规模以上个人信息，加强数据异地容灾备份能力建设，积极应对勒索病毒、数据毁损等事件。

建立完善的数据安全评估机制。各建设单位应按照国家相关法律法规，建立健全平台重要数据和个人信息的安全评估机制，定期组织开展数据安全评估，指导建设单位按照有关要求开展自评估工作。

完善电子认证服务机制。各建设单位应基于合规的电子认证服务实现对电子健康卡系统平台用户的身份鉴别，并结合符合密评要求的密码技术实现对敏感数据操作日志记录的完整性保护，以及其中关键操作的不可否认性保护。此外，还应基于符合密评要求的密码技术和访问控制措施保护重要数据、敏感个人信息的机密性、完整性。

（四）提升监测预警和威胁分析能力

监测预警和威胁分析是平台运行环境亟需提升的重要安全保护能力，加强安全情况及时掌握、风险隐患及时发现、安全事件及时报告，为平台及运行环境安全保护整体水平提升提供技术支撑。

建立平台网络安全监测预警机制。各建设单位应健全完善平台、客户端应用软件及运行环境的监测预警制度，及时掌握汇聚平台的资产、威胁、漏洞、事件等信息，以及平台和客户端应用软件的运行状况、安全态势，加强网络安全风险监测处置工作指导。运营者加强监测预警能力建设，常态化开展网络安全监测工作、报送相关信息，除前文提到的资产、流量安全监测情况外，还应掌握漏洞、事件情况。

建立威胁分析研判机制。各建设单位应探索符合自身实际的方式，重点加强互联网出入口、跨地区跨机构网络入口安全监测，形成技术能力手段，调动技术力量，逐步培养信息安全专业技术人才队伍，主动获取和分析挖掘威胁信息、行动性线索，及时发现对平台进行攻击窃密和破坏的动向，提升威胁信息搜集和分析研判能力。

（五）增强网络安全应急响应水平

各建设单位应建立完善网络安全事件报告制度、应急处置机制，探索应急协调与支援模式，深入开展网络安全应急演练，增强整体网络安全应急响应水平。

（六）提高网络安全检查效能

各建设单位应进一步规范、指导开展常态化检查检测相关工作，对于检查检测发现的安全隐患和风险威胁，督促相关方建立清单台账，逐一制定整改方案，及时开展整改加固，并将整改情况通报检查单位。

（七）提升运维团队安全意识和保障能力

平台运维及监测分析人员应定期统计平台安全运行数据，包括网络安全事件（病毒木马、入侵检测、软件漏洞等）、设备运行情况（磁盘、内存、CPU（Central Processing Unit，中央处理器）使用率等）、系统运行日志（故障、告警等），及时发现并解决电子健康卡系统平台运行中存在的安全问题。

至少每季度组织一次对电子健康卡系统平台运维团队的安全培训，至少每季度一次对运维团队的运维操作进行审查，及时发现、总结、改正问题以提升运维团队安全意识和安全运维能力。

运维团队及监测分析人员需使用专业安全运维工具，确保电子健康卡系统平台的软、硬件运维，事前经授权，事中经审计，事后可追溯取证。

二、电子健康卡系统平台安全架构

（一）电子健康卡应用系统架构

电子健康卡利用电子健康卡跨域主索引及跨域认证系统和电子健康卡管理信息系统（以下简称“卡管系统”），以二维码技术为核心，实现电子健康卡的应用。

电子健康卡系统平台包括以下三部分：

1）符合《电子健康卡建设与管理指南（V3.1）》要求的电子健康卡管理信息系统、电子健康卡密码模块、电子健康卡识读终端；

2）接入电子健康卡的客户端应用软件，包括APP（Application，应用程序）、第三方服务号、自助终端及其他类型的终端等；

3）电子健康卡的受理应用环境，实现电子健康卡在业务应用机构的场景落地。

电子健康卡系统平台架构如图1所示。

注：此图仅表述各系统间的关系，不代表实际的部署架构。

图1　电子健康卡系统平台架构图

在服务端，电子健康卡管理信息系统是电子健康卡的核心系统，具有电子健康卡账户管理、二维码管理、密码服务等功能，并对外部接入的机构、识读终端、客户端应用软件等进行管理。通过电子健康卡跨域主索引实现管辖范围内居民信息统一识别，对所辖各区域居民标识域，以及身份证、社保卡、军官证、港澳居民来往内地通行证、台湾居民来往内地通行证、出生医学证明、就诊卡、护照等标识证的统一注册管理，通过主索引ID进行唯一性标识。通过电子健康卡跨域认证提供在非发卡地进行电子健康卡二维码识别，实现跨地域识别。

在应用端，医疗卫生机构部署机构终端用于申请二维码。机构终端可包括自助终端、挂号窗口终端等多种形式，实现电子健康卡在医疗机构场景的发行。

识读终端用于识读用户提供的二维码，并将二维码信息传输至电子健康卡管理信息系统，用于识别用户身份。

电子健康卡客户端应用软件可注册电子健康卡账户，申请电子健康卡二维码，并可管理与居民健康卡绑定的各医院就诊卡账户，查询居民在各医院的就诊信息。

金融交易机构可接入电子健康卡管理信息系统，作为支付服务提供方，向电子健康卡用户提供支付服务，实现电子健康卡功能与金融支付功能的融合。金融交易机构也可直接与医疗卫生机构建立支付结算通道。

保险机构包括医保机构和商保机构。保险机构作为保险服务提供方，向电子健康卡用户提供保险结算服务，实现电子健康卡功能、金融支付功能、保险结算功能的融合。

电子健康卡系统平台是跨区域、跨机构医疗，实现横纵双向跨域应用、就诊信息共享、医疗大数据的统一入口，是关系到人民群众健康的重要基础设施。

（二）安全架构设计

电子健康卡系统平台安全架构设计主要包括安全技术要求、可靠运行要求、部署安全要求及安全管理要求等。电子健康卡系统平台安全架构如图2所示。

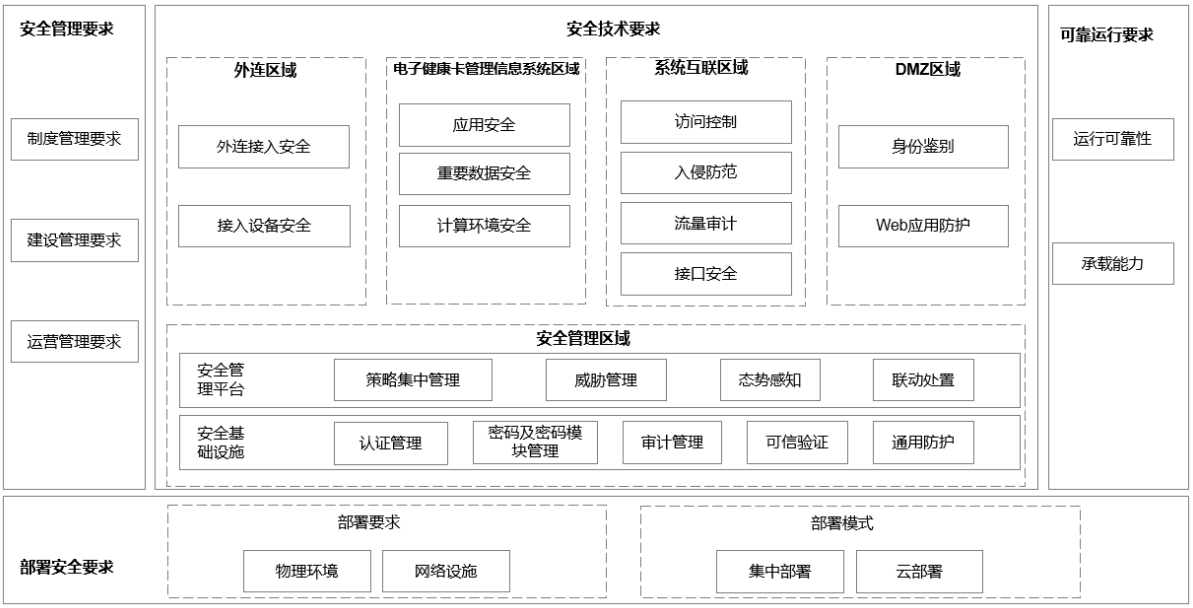

图2　电子健康卡系统平台安全架构组成示意图

安全技术要求将电子健康卡系统平台安全域划分为外连区域、系统互联区域、DMZ（Demilitarized Zone，非军事管理区）区域、电子健康卡管理信息系统区域和安全管理区域。其中，外连区域指主要处理外部访问（个人、医疗机构等）的区域，外连区域安全包含外连接入安全和接入设备安全。DMZ 区域指公布信息的区域，通过互联网接入的外部客户可以访问该区域。DMZ 区域通过用户管理、WEB（网络）防护、身份认证等实现互联网接入用户的访问控制。电子健康卡管理信息系统区域指电子健康卡管理信息系统的部署区域，处理电子健康卡业务逻辑。系统区域安全包含数据安全及计算环境安全。安全管理区域指系统中实现安全基础设施服务和安全运行管理的区域，包括安全管理平台、安全基础设施及业务安全要求。系统互联区域指处理电子健康卡管理信息系统与医疗机构系统、金融机构系统互联的区域，通过访问控制、入侵防范、流量审计、接口安全等实现互联安全。

可靠运行要求包含运行可靠性及承载能力。

部署安全要求包含部署要求及部署方式。

安全管理要求包括制度管理要求、建设管理要求及运营管理要求。

三、安全技术要求

（一）外连区域安全技术要求

1. 外连接入安全

通过互联网、虚拟专网或物理专线实现客户端应用软件及识读终端安全接入电子健康卡系统平台时，应提供通信线路、关键网络设备、关键安全设备和关键计算设备的硬件冗余，保证系统的可靠性。

应采用符合密评要求的密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性；应采用符合密评要求的密码技术保证通信过程中数据的完整性；应采用符合密评要求的密码技术保证通信过程中重要数据的机密性。

应对防火墙进行访问策略配置，仅开放卡管系统必要接口，整体采用白名单机制，按照最小访问控制原则限制外连接入设备网络访问权限。

应对接入设备进行动态检测与控制，对于未通过授权及评估的接入设备应及时阻断、告警。

应对接入流量进行过滤，基于已知的IP（Internet Protocol，互联协议）地址黑白名单对网络流量包、异常请求进行过滤，对命中黑名单的恶意流量进行阻断，并对流量进行安全审计。

应具备针对当前常见主流网络攻击行为的防护能力，包括Flood（泛洪）攻击、扫描或欺骗攻击、畸形报文攻击、反射式攻击等。

应对外连接入用户、设备进行访问控制，默认情况下除允许通信外受控接口拒绝所有通信；应删除多余或无效的访问控制策略，优化访问控制列表，并保证访问控制规则数量最小化；应能基于源地址、目的地址、源端口、目的端口和协议等进行检查，对数据包进行允许/拒绝进出；应能够对进出网络的数据流实现基于应用协议和应用内容的精准识别及灵活控制，可对应用进行策略阻止、会话限制、流量管控、应用引流或时间限制等。

2. 接入设备安全

接入设备安全包括识读终端、自助机和客户端应用软件安全等。

应对接入电子健康卡系统平台的客户端应用软件实行登记制度。客户端应用软件开发完成后，在上线之前，建设单位应向其准备接入的电子健康卡系统平台进行注册登记，并按照《电子健康卡密码模块接口及卡管系统接入认证技术要求》的接入组件编码规则分配登记编号。APP Android、APP iOS、公众号、服务号等每个应用种类均应分配登记编号。

应对客户端应用软件包括APP、小程序、服务号等建立事中安全监测机制及措施。通过主动、持续、动态的风险业务识别、侦测和分析，达到风险识别、预警、处置的风险闭环控制，包括接入的客户端应用软件资产情况、应用合法性监测、安全漏洞监测等。

为保证识读终端设备的身份鉴别和数据加密，应至少采用符合移动端的二级密码模块作为保护，保证自助机、识读终端在数据传输、身份鉴别的过程中，通过数字签名技术对数据进行完整性、一致性的保护；客户端应用软件调用电子健康卡服务时，应使用符合密评要求的密码技术作为身份鉴别手段，保证电子健康卡使用中的身份可信。

（二）DMZ 区域安全技术要求

1. 身份鉴别

应采用符合密评要求的密码技术对访问的用户进行身份标识和鉴别，保证通信实体身份的真实性，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换，应保持相同的用户其用户身份、安全标记、访问控制策略等在不同等级系统、不同业务系统、不同区域中的一致性，例如，可以使用统一身份与授权管理系统/平台。

2. WEB 应用防护

应对DMZ区域提供的对外服务进行WEB攻击防护，有效识别并防御各种WEB威胁，如SQL注入、XSS跨站脚本、CC等恶意网络攻击；支持外链检查、目录访问等WEB防护功能，有效抵御针对WEB服务器的各种安全威胁。WEB应用防护对正常访问造成的性能损失不应超过10%。应对身份验证Cookie的内容进行加密，如果Cookie信息包含了身份验证信息，则必须对Cookie内容进行加密。

应对DMZ区域提供的对外服务进行API攻击防护，检测、识别、拦截针对API接口的攻击。

应对DMZ区域提供的对外服务进行应用层DDoS攻击防护，阻断恶意发送大量合理请求、消耗目标系统服务资源的DDoS攻击行为。防DDoS攻击的能力宜不小于平台接入带宽的50%。可防护攻击种类应覆盖所有已知的DDoS攻击类型，如SYN Flood，ICMP Flood。

（三）卡管系统区域安全技术要求

1. 应用安全

（1）身份鉴别

应采用符合密评要求的密码技术对终端用户登录、终端管理系统登录及其他系统级应用登录进行身份鉴别，保证通信实体身份的真实性，身份标识具有唯一性。

卡管系统应对账户口令有强制性的复杂度限制，对于复杂度不符合要求的口令，无法被平台所接受；平台登录账户及口令应配置口令定期强制更换安全策略，强制用户定期更换口令，否则无法登录，口令更换周期最长不应超过一个月。

应具有账号登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。

应保持相同的用户其用户身份、安全标记、访问控制策略等在不同等级系统、不同业务系统、不同区域中的一致性，例如，可以使用统一身份与授权管理系统/平台。

应采用动态口令、符合密评要求的密码技术、生物技术等多因子身份鉴别方式对用户进行身份鉴别，且其中一种鉴别技术至少应使用符合密评要求的密码技术来实现。对于重要业务操作或异常用户操作行为，应建立动态的身份鉴别方式。

（2）安全访问机制

应对登录的用户分配账户和权限；重命名或删除默认账户，修改默认账户的默认口令；应及时删除或停用多余的、过期的账户，避免共享账户的存在；应授予管理用户所需的最小权限，实现管理用户的权限分离。

卡管系统应采取强身份认证、授权管理、访问控制措施，限制非授权用户对系统级资源的访问。

（3）数据备份要求

系统应实现数据备份功能，所有静态数据表和录入的资料在运行机器外应有一个数据库的备份和一个通用格式文件的备份。

应采用增量备份方式对平台的数据进行备份，每日发生数据变更应在运行机器外至少保存有数据库的增量备份和对应的通用格式文件的备份，保证平台的数据可以回滚恢复到故障发生前1小时的状态。

（4）系统配置管理安全要求

应确保配置管理界面的安全，仅允许经过授权的操作员和管理员访问，在管理界面上实施强身份验证，如使用证书等。

（5）通信管理要求

卡管系统和客户端应用软件在外部传输时应采用安全传输协议，宜采用符合密评要求的密码技术建立安全的信息传输通道。

应对身份验证Cookie的内容进行加密；如Cookie信息包含了身份验证信息，则应使用密码算法对Cookie内容进行加密。

（6）终端管控

终端应安装、注册并运行终端管理客户端软件。

终端应接受电子健康卡系统平台终端管理服务端的设备生命周期管理、设备远程控制、设备安全管控。

（7）应用管控

应具有软件白名单功能，应能根据白名单控制应用软件安装、运行。

应具有应用软件权限控制功能，应能控制应用软件对终端中资源的访问。

应只允许电子健康卡系统平台管理者指定证书签名的应用软件安装和运行。

应具有接受终端管理服务端推送的应用软件管理策略，并根据该策略对软件实施管控的能力。

（8）资源控制

应将终端处理访问电子健康卡系统平台的运行环境与非处理访问电子健康卡系统平台运行环境进行系统级隔离。

应限制用户或进程对终端系统资源的最大使用限度，防止终端被提权。

宜采用符合密评要求的密码技术保证信息系统应用的重要信息资源安全标记的完整性。

在可能涉及法律责任认定的应用中，宜采用符合密评要求的密码技术提供数据原发证据和数据接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性。

2. 重要数据安全

（1）电子健康卡系统平台重要数据内容

电子健康卡系统平台重要数据包含鉴别数据、重要业务数据、审计数据、主要配置数据、重要个人信息等内容。

电子健康卡系统平台外部数据源包括电子健康卡系统平台主要配置数据和重要业务数据。

（2）电子健康卡系统平台重要个人信息采集规则

电子健康卡系统平台重要个人信息采集规则包括：

a) 个人信息机构端采集：用户提供个人身份认证证件（如：身份证），由医疗机构端进行个人身份信息采集以及实名认证，实名认证通过后，提交个人信息到电子健康卡系统平台。

b) 个人信息客户端应用软件采集：用户通过客户端软件到第三方实名认证系统进行实名认证（如：公安信息系统），实名认证通过后，提交个人信息到电子健康卡系统平台。

（3）数据收集安全要求

重要数据在收集阶段要遵循如下安全要求：

a) 应定义重要数据的采集规则，如采集原则、采集渠道等，以保证该业务数据采集的合法性和正当性，应确保重要数据的采集只限于实现处理目的的最小范围，不过度收集其他信息。

b) 收集重要数据应当采取合法、正当、必要的方式获取数据。应结合具体管理、业务场景，制定重要数据收集规则，规范重要数据收集渠道、数据格式、收集流程和收集方式，定期开展重要数据收集合规性审查。

c) 数据采集应当遵循应当采取合法、正当的方式，确保数据采集的准确性、完整性、时效性，不得窃取或者以其他非法方式获取数据，同时，要明确数据采集的目的、范围、用途，明确数据采集的渠道、流程和方法。

d) 在使用数据共享平台时，数据采集应向数据提供方提交数据采集申请，同意后开展采集工作。

e) 委托第三方机构采集数据时，须签订保密协议。要求其不得超出最小授权范围，不得违规存储、加工、使用所采集的数据。

f) 数据采集环境、采集设施和采集技术手段应安全可控。

g) 针对外部数据源，应要求外部数据提供方说明数据来源，审核外部数据提供方的身份，并对数据来源的合法性进行确认，留存审核、交易记录，确保数据收集渠道的合法性和正当性。

h) 应规定数据采集的渠道及外部数据源鉴定方式，并对采集来源方式、数据范围和类型进行记录，

确保不收集与提供服务无关的个人信息。

i) 应明确重要数据采集安全管理要求，包括组织采集数据时的原则，定义业务数据的直接或间接采集流程和方法。

j) 如有直接面向客户采集数据的业务场景，负责该业务的部门应根据国家相关法律规定制定面向客户的隐私保护协议。

k) 应规定数据采集过程中个人信息的知悉范围和需要采取的控制措施，确保采集过程中的个人信息不被泄露，尤其是重要个人信息。

l) 应明确重要个人信息采集需要用户授权同意。

m) 应明确外部数据源已获得的个人信息处理的授权同意范围，包括使用目的、采集范围、个人信息主体是否授权同意共享等。

n) 收集重要数据过程中，应当采取配备技术监测手段、签署安全协议、账号权限管控、监督审核、审计等措施加强对重要数据收集人员、设备系统的管理，并对重要数据收集的时间、类型、数量、频度、流向等进行记录。

o) 应对重要数据收集所涉及的软硬件工具、设备、系统、平台、接口以及收集技术等，应采取必要的测试、认证、鉴权等措施，并进行内部审批。

p) 在收集重要数据过程中采取相应的技术手段，防止数据在收集过程中被泄露。

q) 应建立数据采集工具，具备详细的日志记录功能，保障数据采集授权过程的完整记录，并对数据采集过程的可追溯。

r) 在收集重要数据过程中如果需要缓存，应具备数据加密存储能力，并在完成数据收集时及时清除缓存。

s) 应采用口令、设备指纹、设备物理位置、网络接入方式、设备风险情况等多种因素对数据收集的设备或系统的真实性进行校验。

t) 收集重要数据过程中，出现违反法律法规或相关标准要求的情况，应立即停止收集活动并按要求向网信部门和有关部门报告。

（4）数据传输安全要求

重要数据在传输阶段要遵循如下安全要求：

a) 应根据合规要求和业务性能的需求，明确核心业务汇总需要加密传输的数据范围和密码算法。

b) 系统之间的通信应采用符合密评要求的密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性、完整性、可追溯性。应采用符合密评要求的密码技术对通信实体的传输数据进行加密，保证通信过程中数据的机密性。

c) 在数据分类分级定义的基础上，应制定数据传输安全管理规范，明确各业务场景下的数据传输安全要求。

d) 应根据业务流程、职责界面、网络部署、安全风险等情况，合理划分网络系统安全域，区分域内、域间等不同数据传输场景，明确重要数据传输安全策略和操作规程。业务管理人员和安全技术人员应对重要数据传输安全策略和操作规程的变更进行审核和监控，包括对密钥使用、传输通道及接口安全配置、密码技术选择、传输协议升级等技术保护措施的审批及监控。

e) 应建立数据传输安全策略变更审核和监控制度。

f) 采用物理介质传输重要数据时，应采用密码硬件设备的方式，设备宜默认开启数据加密功能。传输后应及时从设备销毁数据，并确保重要数据不能被恢复。

g) 应提供对数据传输安全策略的变更进行审核和监控的技术方案和工具。

h) 应建立重要数据传输接口安全管理工作规范，明确技术管控措施。对涉及重要数据的接口调用实施控制，包括流控制、流量监控、调用过载保护等，定期对接口权限控制、传输等相关功能进行安全评估，核实安全措施的有效性。

i) 应在数据导入导出过程中配备安全技术手段，防止数据的可用性和完整性遭到破坏。

j) 平台在公共网络链路上传输时，应采用加密形式；数据加密应采用 128bit 或以上的密钥；重要数据机密性应采用符合密评要求的密码算法。

（5）数据访问控制安全要求

重要数据在访问控制方面要遵循如下安全要求：

a) 核心业务应明确重要系统和数据库的身份鉴别、访问控制和权限管理的安全要求。

b) 应明确数据权限授权审批流程，对数据访问权限申请和变更进行审核。

c) 应明确对身份标识与鉴别、访问控制及权限的分配、变更、撤销等方面管理的要求。

（6）数据存储安全要求

重要数据在存储阶段要遵循如下安全要求：

a) 重要数据应存储在中华人民共和国境内。

b) 重要数据应进行分类存档。

c) 应定期检查数据存储系统安全配置以符合基线的一致性要求。

d) 应定期探查存储系统的数据是否符合相关合规性的要求。

e) 应支持符合密评要求的密码算法，对高敏感数据进行加密存储；系统的密钥数据须存储在硬件密码设备内的，密钥不以任何形式出现在硬件密码设备以外。

f) 应明确重要数据存储安全策略和操作规程，包括重要数据存储平台系统的安全存储保护措施（如符合国家法律、法规的规定和密码相关国家标准、行业标准有关要求的密码技术、校验技术、数字签名、访问控制、日志管理、安全审计、版本升级等）、数据存储介质安全管控策略和管理规定等；与系统支撑运维人员签订数据安全协议，有效约束操作行为。

g) 应建立重要数据存储安全的制度规范，对存储环境变更、存储介质、逻辑存储访问控制规则进行基本约束。

h) 应提供工具支撑存储介质及逻辑存储空间的安全管理工作，提供如权限控制、存储空间的身份鉴别、逻辑访问控制以及运维管理的基本能力。

i) 应建立存储介质及逻辑存储管理遵循的安全管理制度体系，包括电子健康卡数据安全管理政策、实施细则及指导方案，尤其是重要个人健康信息存储相关管理细则。

j) 应依据最小够用原则存储重要数据，不应以任何形式存储非必需的重要数据，存储时间应为业务必需的最短时间，国家及有关主管、监管部门另有规定的除外。

k) 重要数据的存储平台系统、相关数据处理及传输设备应部署于安全域内，不直接提供公共信息网络访问。

l) 应加强对重要数据处理相关平台系统接入移动存储介质的管控，针对将重要数据下载到本地终端和向移动介质输出重要数据的行为进行严格控制。

m) 应建立存储介质的保存环境制度规范，明确存储介质引入流程、出入库规范、保存环境要求、以及可用性保障要求。

n) 应具备重要数据完整性校验手段，支持对存储重要数据完整性的检查，能够发现重要数据存储过程中的丢失或损坏，并具备相应的恢复措施。

o) 应提供逻辑存储的安全配置检查技术手段，定期进行安全配置检查。

p) 应明确重要数据容灾备份的规范和操作规程，包括数据备份周期、备份方式、备份地点、数据恢复性验证机制等内容，保障数据的可用性和完整性；一旦发生数据丢失或破坏，确保能够利用备份及时、完整、准确的恢复数据。

（7）数据使用加工安全要求

重要数据在使用加工阶段要遵循如下安全要求：

a) 应对重要数据的使用加工建立严格的审批流程，确保重要数据在国家法律法规允许的范围内使

用加工，不影响国家安全、社会公共利益；明确在使用加工过程中的数据获取方式、访问接口、授权机制、物理和逻辑安全、处理结果安全等策略和操作规程，并周期性的检查用户使用数据的情况。

b) 应依据最小使用原则开放数据的使用和加工，确定数据使用加工的场景、范围和权限规则。

c) 在重要数据使用加工过程中应确保重要数据的使用加工不超过原始数据的授权范围和安全使用加工要求，严格控制单个数据使用加工任务中允许使用的数据规模和范围。

d) 应保证数据加工操作的规范化、自动化，采用相同标准、统一的方式进行数据加工，并对重要数据提供痕迹保留、数据追踪和防范非法扩散的功能。

e) 在使用加工重要数据时，从账号身份管理、身份凭证保护、最小授权原则、数据权限设置等方面落实重要数据访问控制措施，统一管理数据使用权限，建立登记、审批机制并留存记录。

f) 应结合具体业务，明确重要数据脱敏处理使用应用场景，建立重要数据脱敏处理管理规范和制度，明确重要数据脱敏规则、脱敏方法、数据脱敏处理流程，不得将未脱敏的重要数据用于系统的开发测试。

g) 宜在合适场景下采取隐私保护技术实现数据不出域使用。

h) 应结合系统和业务管理，同步建立技术手段或机制，对违规使用加工重要数据的行为进行有效的识别、监控和预警。

i) 在重要数据使用加工过程中，发现可能危害国家安全、公共安全、经济安全和社会稳定的较大安全风险时，应立即停止使用加工活动并按要求向有关部门报告。

j) 应采取必要措施提升数据溯源能力（如对数据进行签名、添加数字水印等），防止重要数据被恶意删除、随意篡改和滥用。

k) 在用户终端显示平台的数据时，应采用去标识化操作，防止个人敏感信息的泄露。

（8）数据提供安全要求

重要数据在提供阶段要遵循如下安全要求：

a) 对数据接收方的数据安全保护能力和资质进行核实，并与数据接收方签订数据安全协议，明确数据提供的范围、使用方式、时限、用途、相应的安全保护措施、违约责任以及不慎泄露的应急方案，并督促数据接收方予以落实。对提供的重要数据，应当采取数据脱敏等措施。

b) 建立重要数据提供的安全审核制度，审核提供的重要数据内容，对重要数据提供进行有效控制，确认没有超出需求和授权范围的数据。重要数据提供的审批记录、日志记录至少留存五年。

c) 应对重要数据提供的终端、用户、接口或服务组件执行有效的访问控制，实现对其身份的真实性和合法性的验证。

d) 应对开放接口进行有效管理，记录接口的访问参数（如账号、访问时间、访问内容等），防止重要数据滥用、重要数据窃取等行为；定期对开放接口进行清查，对不符合要求的接口立刻予以关停。

e) 宜在合适的场景下采取隐私保护技术实现以可用不可见的方式对外提供数据。

f) 应采取必要措施提升数据溯源能力（如对数据进行签名、添加数字水印等），确保能对提供出去的数据进行溯源。

（9）数据外部共享安全要求

重要数据在外部共享阶段要遵循如下安全要求：

a) 应明确数据外部共享的原则、范围和安全规范，明确数据外部共享内容范围和数据外部共享的管控措施，及数据外部共享涉及机构或部门相关用户职责和权限。

b) 应与数据外部共享方签署保密和合作协议，明确数据的使用目的、供应方式、保密约定、数据安全责任等。

c) 应保证共享内容符合数据合规和监管要求，明确数据挖掘和应用范围。

d) 应制定数据外部共享的原则及数据保护措施，尤其是个人信息的外部共享，应在个人信息使用许可前提下确保数据使用的相关方具有对共享数据的足够的保护能力，从而保障数据共享安全策略的有

效性。

（10）数据销毁安全要求

重要数据在销毁阶段要遵循如下安全要求：

a) 应建立重要数据销毁安全策略和操作规程，明确销毁对象、原因和流程、存储介质销毁处理、技术等要求，对销毁活动进行记录和留存。

b) 应建立重要数据销毁审批机制，对重要数据销毁过程开展监督，确保两人以上在场，并在事后对销毁情况进行检查核实。

c) 应选择符合国家安全规范的数据销毁方式对重要数据进行销毁。

d) 应以不可逆方式销毁数据，数据销毁完成后，应及时向相关主管部门更新备案，不得以任何理由、任何方式对销毁的重要数据进行恢复。

3. 计算环境安全

（1）主机安全

应对恶意代码及垃圾邮件进行实时检测、查杀或隔离。

应对主机网络连接的端口、协议类型等进行有效管理，关闭不需要的系统服务、默认共享和高危端口，阻断未知协议。

应对主机系统安全极限进行核查，包含账号与口令检查、口令生存周期检查、远程登录检查、网络与服务检查、日志审计检查、防火墙检查、系统安全配置检查等内容，并根据基线核查结果，进行主机安全评估，对评估不合格项应及时处置。

应通过采集、分析主机数据，发现存在风险和威胁的主机。

应能检查并调整主机操作系统的安全策略和配置。

应对主机重点操作如重启、关机、配置更新、文件删除、修改等进行审计，并保留相关审计记录。

应能扫描、分析主机上存在的安全漏洞，及时响应确认并整改主机漏洞、WEB漏洞、渗透漏洞、零日漏洞预警。

应实时监控、识别针对主机的入侵和病毒攻击行为并阻断。

宜采用符合密评要求的密码技术对主机重要可执行程序进行完整性保护，并对其来源进行真实性验证。

宜采用符合密评要求的密码技术保证设备中的重要信息资源安全标记的完整性。

可采用微隔离技术，基于通信协议、IP、端口、防护动作等细粒度进行主机间东西向访问控制。

（2）云主机安全

应采用白名单、黑名单或其他方式，在网络出入口以及系统中的主机、移动计算设备上实施恶意代码防护机制。

应通过对云主机进行基线核查、漏洞扫描、入侵检测、安全加固、安全迁移、恶意代码查杀，对镜像进行安全加固、漏洞扫描、访问控制、安全备份，提高云主机安全防护能力，保障镜像数据安全；能够对云主机主动散播和被操纵主机的被动有害信息散播行为进行检测和防护、清除并告警。

宜使用数据挖掘防范和检测技术，检测和防范对数据存储介质的数据挖掘。

（四）安全管理区域安全技术要求

1. 安全基础设施

（1）认证管理

应在设备接入、网络互联、系统访问时进行身份认证。

应对设备建立动态的身份认证方式，或者采用口令、符合密评要求的密码技术、生物技术等多因子身份认证方式，且其中一种认证技术至少应使用符合密评要求的密码技术来实现。

在电子健康卡系统平台PC（Personal Computer，个人计算机）端/移动端使用硬件介质证书/移动端证书，在网络接入边界部署安全认证网关，在系统基础设施部署数字证书认证系统、手机盾系统或SIM盾系统，通过向相关用户配发数字证书，实现对PC端/移动端登录应用用户的安全身份鉴别，防止非授权人员登录。保证应用系统的访问安全和传输数据的加密安全。

（2）密码模块管理

密码算法应采用国家密码管理主管部门批准使用的密码算法。

电子健康卡系统平台所应用的密码模块必须具有商用密码产品认证证书。

（3）审计管理

应配置具有安全审计功能的设备或系统对电子健康卡系统平台的应用、主机、数据库、网络流量进行审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。

应对电子健康卡系统平台的运行状况、网络流量、用户访问操作行为等进行日志审计记录；审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；应对审计进程进行保护，防止未经授权的中断。

审计记录留存时间应不少于12个月。

宜采用符合密评要求的密码技术保证审计记录的完整性。

（4）可信验证

可基于可信计算技术，采用白名单机制，对重要应用或主机提供执行程序可信度量、恶意代码防御机制及可信目录标识，阻止非授权及不符合预期的执行程序运行，实现对已知/未知恶意代码的主动防御，构建可信目录可以保证运行某些程序时产生的临时文件的正常运行，通过路径识别将可信目录下的所有进程版时加入白名单，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理平台。

（5）通用防护

应提供针对电子健康卡系统平台的基础安全防护能力，包括安全识别、安全防护、安全检测、安全响应等。

安全识别能力包括但不限于资产发现、漏洞扫描、基线核查等能力。

安全防护能力包括但不限于访问控制、隔离交换、设备准入、入侵防御、恶意代码查杀、补丁管理、应用安全防护等能力。

安全检测能力包括但不限于威胁检测、恶意代码检测、数据泄露检测等能力。

安全响应能力包括但不限于攻击溯源、调查取证、响应恢复等能力。

2. 安全管理平台

（1）策略集中管理

应支持安全策略的集中管理，支持从外部设备/系统获取相关数据，结合安全风险、告警、威胁情报等信息实现安全策略的优化。

（2）威胁管理

应具备多维分析能力，综合多种信息元素进行全局网络的流量分析、日志分析以及关联分析，深度挖掘潜在的威胁行为，还原攻击路径，发现攻击意图；威胁分析应至少包含主机威胁及业务威胁；应支持威胁事件的告警。

应安装防恶意代码软件，定期对运维管理终端、主机和网络设备进行扫描，及时更新防恶意代码软件版本和恶意代码库。

（3）态势感知

应支持对电子健康卡系统平台内资产、安全事件、安全风险、安全威胁等信息进行采集、分析、展示。

应支持对电子健康卡系统平台进行被动式全网信息采集和主动式扫描探测，对安全态势进行分析、检测和可视化态势分析展示，包括综合安全态势、外部攻击态势、资产安全态势、威胁事件态势、弱点态势等。

（4）联动处置

应支持威胁告警，告警方式包括电子邮件、声音提醒、短信等多种方式。

可制定基于资产、事件、风险等级等维度的自动化编排响应处置机制，当出现安全事件时，安全人员可根据预定义的工作流程，确定优先级并推动标准化的事件响应活动，快速定位问题并第一时间进行响应。

（五）系统互联区域安全技术要求

1. 访问控制

应部署逻辑隔离设备进行访问控制，当外部机构通过虚拟专网或物理专线接入电子健康卡系统平台时，可有效过滤病毒、木马、蠕虫、间谍软件、漏洞攻击、逃逸攻击等安全威胁，提供L2-L7层网络的全面安全防护。

应采用符合密评要求的密码技术保证电子健康卡系统平台应用的重要数据在传输及存储过程中的机密性。重要数据宜采用量子密钥加密。

宜采用符合密评要求的密码技术保证系统资源及应用访问控制信息的完整性。

宜采用符合密评要求的密码技术保证信息系统应用的重要数据在传输及存储过程中的完整性。

2. 入侵防范

应采取入侵检测与防护措施，防止攻击者利用平台的漏洞，在平台的系统中植入后门程序。

应采用行为分析的方法，有效发现针对平台的入侵行为。

应采用模拟平台诱骗攻击的技术，发现针对平台的早期入侵行为。

应利用外部威胁情报，提升入侵行为检测的准确度。

应采用终端安全防护措施，及时发现平台服务器主机上的异常行为，防止平台服务器被植入恶意程序。

3. 流量审计

应对外部机构与电子健康卡系统平台的访问流量进行采集、记录和分析，对主流的应用软件、文档文件、媒体文件及压缩文件进行恶意代码检测审计，及时发现未知威胁（如APT攻击）。

4. 接口安全

接口服务提供方应提供接口技术规范，包括调用方式、参数、封装格式、合法性校验等内容。

应采用技术措施，对平台的应用程序接口（API）进行防护，防止高频访问等针对平台API的恶意调用。

所有接口业务数据应使用国家密码管理主管部门批准的密码算法实现抗抵赖、完整性和保密性保护。

应对外部接口服务的访问次数、时间、速率、每日增量等进行控制。

宜建立标准服务系统，提供统一应用接入进行集中安全管理和分发，包括服务申请管理、审批管理、应用接入管理、使用情况统计查询等。

四、可靠运行要求

（一）运行可靠性

为保障电子健康卡系统平台安全平稳运行，建设单位应确保电子健康卡在使用期间对于电子健康卡注册、生成二维码和验码功能的安全稳定运行，年均不间断运行时间应达到90%总时间，宜达到99%总时间，有条件的单位建议达到99.9%总时间。

电子健康卡管理系统数据库应具有备份机制，系统涉及到的数据库表均应有不超过24小时的定时备份，宜采用主从模式或者其他方式实现实时备份。

电子健康卡系统平台应建立热备或双活机制，具备在紧急情况下第一时间进行快速切换的能力，保证在以下情况下不丢失数据：1）容量达到规定的极限；2）容量超出规定的极限；3）使用者不正确的输入；4）系统死机；5）关键硬件出现故障。

关键网络节点和计算节点应具备冗余机制，包括服务器、防火墙设备、交换机设备、密码设备、安全产品等。

电子健康卡系统平台应具有灾备能力，数据灾备恢复RTO（恢复时间目标）应不大于4小时，RPO（恢复点目标）应不大于6小时。

应对客户端应用软件建立主动、持续、动态的安全风险监测机制及措施。

应建立全链路的监控体系，进行网络、计算、存储、数据库、接口调用、安全等模块的运行情况进行集中统一监控，并在指标出现异常时及时告警并快速处置，监控告警方式可包括微信告警、短信告警、电话告警、邮件告警等。

应具备对服务器磁盘、CPU、内存使用率、网络带宽、数据库占用资源、慢查询情况的监控可视化界面。

应实现生产环境与其他环境（包括但不限于开发环境、测试环境、预发环境）的隔离。

应建立测试验证环境，系统重大版本上线前应对功能、性能等进行充分的测试验证。系统新版本上线后若发现故障，应能够快速回滚，确保数据不丢失。

电子健康卡管理信息系统应对内部接口和外部接口进行分类管理，在外部接口故障时，可通过停止或减少外部接口调用等方式避免影响系统稳定运行。

应定期升级使用的服务组件、中间件等软件和应用程序。

应采取限流、排队、服务端缓存、手机客户端缓存、内容分发网络（CDN）、用户刷新频率限制等技术措施，加强应对突发尖峰流量冲击的能力。

（二）承载能力

电子健康卡管理信息系统运行于单台服务器/节点进行电子健康卡注册、申请二维码、验证二维码操作时应满足并发用户数不低于1000个，平均响应时间不高于3秒，事务成功率不低于99%，应用及数据库服务器CPU、内存资源利用率不高于75%。

电子健康卡管理信息系统应根据部署地常住人口与系统历史最大并发数等因素，评估确定合理容量，每秒最大完成请求数应满足部署地常住人口的千分之一，建议达到部署地常住人口的千分之二；在用户并发执行电子健康卡注册、申请二维码、验证二维码操作时，通过电子健康卡应用监测平台定时采集并

取平均值获取的响应均值应在1000毫秒内，成功率应达到100%；建议有条件的单位将响应均值控制在500毫秒以内。

在应急情况下，系统宜达到4小时内自动或手动增加应用服务节点数，从而满足应急所需访问诉求。

五、部署安全要求

（一）部署要求

1. 物理环境要求

（1）物理位置选择

机房场地应选择在具有防震、防风和防雨等能力的建筑内。

机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。

（2）物理访问控制

机房出入口应配置电子门禁系统、有专人值守的视频监控系统，控制、鉴别和记录进出的人员，电子门禁系统和视频监控系统应采用符合密评要求的密码技术，保证进出人员身份的真实性，以及进出记录数据和视频监控音像记录数据的完整性。

（3）防盗窃和防破坏

应将设备或主要部件进行固定，并设置明显的不易除去的标识。

应将通信线缆铺设在隐蔽安全处。

应设置机房防盗报警系统或设置有专人值守的视频监控系统。

（4）防雷击

应将各类机柜、设施和设备等通过接地系统实现安全接地。

应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。

（5）防火

机房应设置烟感报警装置及火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火。

机房及相关的工作房间和辅助房间应采用具有耐火等级的建筑材料。

（6）防水和防潮

应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透。

应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。

应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。

（7）防静电

应采用防静电地板或地面并采用必要的接地防静电措施，同时应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。

应定期使用吸尘器对机房进行打扫，机房进出入口应放置防尘地毯贴，或准备相应的防尘穿戴物件供进出人员使用。

（8）温湿度控制

应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。

（9）电力供应

应在机房供电线路上配置稳压器和过电压防护设备。
应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。
应设置冗余或并行的电力电缆线路为电子健康卡系统平台供电。

（10）电磁防护

电源线和通信线缆应隔离铺设，避免互相干扰。
应对关键设备实施电磁屏蔽。

2. 网络设施要求

（1）网络架构

接入设备的处理能力应满足业务高峰期需要。
应采用符合密评相关要求的安全接入设备，实现身份鉴别和通信数据加密功能。

（2）边界防护

应部署安全接入网关设备，实现网络之间边界防护。

（3）访问控制

应根据访问控制策略设置访问控制规则，默认情况下，除允许通信外，受控接口拒绝所有通信。
应对流入的数据流量、数据包和协议等进行检查，以允许/拒绝数据包通过。
应在接入网关上对进出网络的数据进行内容过滤。
应设置访问控制规则限制可访问的对象资源。

（4）入侵防范

应能够检测、记录、定位非授权无线接入设备及非授权终端接入。
应具备对针对接入设备的网络扫描、DoS攻击（Denial of Service，拒绝服务攻击）、密钥破解、中间人攻击和欺骗攻击等行为进行检测、记录、分析定位。
应能够检测到接入设备的SSID（Service Set Identifier，服务集标识）广播、WPS（WiFi Protected Setup，WiFi保护设置）等高风险功能的开启状态。

（5）通信传输

应采用国家密码管理主管部门批准使用的密码算法保证通信过程中数据的完整性。
应采用国家密码管理主管部门批准使用的密码算法保证通信过程中敏感信息字段或整个报文的保密性。

（6）安全审计

应启用网络设备及安全设备的安全审计功能，审计覆盖到登录网络设备和安全设备的管理员用户，对重要的终端行为和重要安全事件进行审计。
应能对终端接入的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。

（7）网络设备防护

应能发现系统移动终端、接入设备、接入网关设备可能存在的漏洞，并在经过充分测试评估后，及时修补漏洞。

应禁用接入设备和接入网关存在风险的功能，如：SSID广播、WEP（Wired Equivalent Privacy，有线等效保密）认证等。

应禁止多个AP（Access Point，接入点）使用同一个鉴别密钥。

（二）部署模式

电子健康卡系统平台应支持多种部署模式，满足省级部署、地市级部署、医疗机构部署、跨区域部署等多种场景的要求。

1. 集中部署模式

各建设单位应强化管理责任，完善管理手段，落实管理措施；应建设同城或者异地的灾备系统，以支撑电子健康卡的实际应用。

系统归属部门应增强安全保密意识和技能，掌握电子健康卡安全运维的技术，维持电子健康卡安全运行的管理工作。

卡管系统及数据库宜部署在不同的网段区间内；卡管系统和数据库均应部署在卡管系统区域，其他系统可部署在DMZ区或外连区，实现网段隔离。

2. 云部署模式

采用云部署模式的建设单位应确保云计算服务器及运行关键业务和数据的物理设备位于中国境内。

电子健康卡系统平台应符合SaaS化要求，且其与密码机之间的数据交互安全应符合等保第三级和密评第三级的要求。

采用容器云部署模式的，容器化部署应不小于3个节点，并采用应用集群的部署方式。

应保障应用系统和数据的安全，确保平台主机发生迁移后，原物理服务器应彻底清除已迁移系统主机的全部数据。

应保证密码机与云端服务器数据传输的安全性。

应采用通过云计算服务安全评估，以及等保第三级或以上等级测评的云计算平台。

六、安全管理要求

（一）制度管理要求

1. 安全制度及策略制定

各建设单位应将电子健康卡系统平台安全管理制度及安全策略纳入网络安全工作的总体方针和安全策略中。

电子健康卡系统平台安全管理制度包括但不限于：网络和系统安全管理制度、风险管理制度、网络安全考核及监督问责制度、网络安全教育培训制度、人员管理制度、资产、配套设施及软硬件维护管理制度、业务连续性管理及容灾备份制度、安全事件报告和处置管理制度、三同步制度、供应链安全管理制度、密码应用安全管理制度等。其中，密码应用安全管理制度应包括密码人员管理、密码管理、建设运行、应急处置、密码软硬件及介质管理等。

电子健康卡系统平台安全策略包括但不限于：安全互联策略、安全审计策略、身份管理策略、入侵防范策略、数据安全防护策略、自动化机制策略（配置、漏洞、补丁、病毒库）、供应链安全管理策略、安全运维策略、口令更新策略、系统变更策略、数据的备份策略和恢复策略等。其中，供应链安全管理策略包括：风险管理策略、供应商选择和管理策略、产品开发采购策略等。

应定期对安全管理制度和密码应用安全操作规程的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。

2. 授权和审批

应针对电子健康卡系统平台的系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度；应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。

3. 审核和检查

应定期对电子健康卡系统平台进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。

应定期对电子健康卡系统平台进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等。

应制定安全检查表格实施安全检查，对电子健康卡系统平台服务器资源、采集、查询、告警信息、硬件状态等进行监控和巡查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。

（二）建设管理要求

1. 三同步原则

安全保护措施应当与电子健康卡系统平台同步规划、同步建设、同步使用。

2. 识别认定

电子健康卡系统平台中，电子健康卡管理信息系统、电子健康卡跨域主索引及跨域认证系统应被识别认定为关键业务。

关键业务所依赖的资产及外部资产，包括网络、系统、服务、接入到电子健康卡系统平台的客户端应用软件/机构终端及其他资产应建立资产清单并定期核对更新。

应对关键业务及关键业务所依赖的资产的分布及运营情况进行跟踪和自动化管理。

3. 安全方案设计

应按照GB/T 22239的第三级要求、GB/T 39786的第三级要求及要求进行安全方案设计。

应根据商用密码相关标准和密码应用需求，制定商用密码应用方案并按照应用方案实施建设，应根据密码应用方案，确定系统涉及的密钥种类、体系及其生存周期环节，各环节密钥管理要求参照GB/T 39786相关内容。

应根据GB/T 36635-2018等要求，完善平台、客户端应用软件及运行环境的监测设计方案，设计常态化网络安全监测工作。

4. 供应链安全保护

应确保网络安全产品采购和使用符合国家的有关规定。

应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求；如采用密码服务，该密码服务应符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格；采用的密码产品，应达到GB/T 37092二级及以上安全要求。

应优先采购安全可信的网络产品和服务。采购网络产品和服务可能影响国家安全的，应当按照国家网络安全规定通过安全审查。

采购网络产品和服务，应当按照国家有关规定与网络产品和服务提供者签订安全保密协议，协议内容应包括安全职责、保密内容、奖惩机制、有效期等，明确提供者的技术支持和安全保密义务和责任，并对义务和责任履行情况进行监督。

宜优先采购基于国产CPU、国产操作系统等信息创新软硬件产品，例如采用符合GB/T 33190-2016的版式文件格式。

5. 软件开发

应在卡管系统、客户端应用软件等软件产品交付前检测其中可能存在的恶意代码。
应保证开发单位提供软件设计文档和使用指南。
应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽通道。

6. 项目实施

应指定或授权专门的部门或人员负责项目实施过程的管理。
应制定安全工程实施方案控制项目实施过程。
应通过第三方工程监理控制项目的实施过程。

7. 测试验证要求

应对平台进行渗透测试和源代码审计，并在经过充分测试评估后，及时修补漏洞；漏洞修复后，应进行复测，验证漏洞是否已经被修复。
应对平台进行压力测试，压力测试所模拟的并发访问数量应不小于系统设计所约定的性能参数。

8. 系统交付

应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点。
应对负责运行维护的技术人员进行相应的技能培训。
应提供建设过程文档和运行维护文档。

9. 等保测评及密评

系统投入使用前应该按照第三级要求完成等保测评和密评，评估通过后系统方可正式运行。
应每年一次进行等保测评及密评，发现不符合相应保护标准要求的及时整改。应在发生重大变更或级别发生变化时进行测评及评估。
应确保测评及评估机构的选择符合国家有关规定。

10. 服务供应商选择

应确保电子健康卡系统平台运维服务、安全服务等服务供应商的选择符合国家的有关规定。
应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。
应定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。

（三）运营管理要求

1. 资产管理

应编制并保存与电子健康卡系统平台相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。
应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施。
应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。

2. 介质管理

应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点。
应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。

3. 设备维护管理

应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理。

信息处理设备应经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据应加密。

含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用。

确保优先使用已登记备案的运维工具，如确需使用由维护人员带入电子健康卡系统平台内部的维护工具，应在使用前通过恶意代码检测等测试。

4. 系统维护管理

为保证电子健康卡中所涵盖的数字证书、密码设备、安全设备可用性、易用性，应建立完整的安全运营管理体系，保证电子健康卡的业务连续性不因数字证书、密码设备、安全设备造成的性能压力问题而导致延迟以及中断，应采用线上或者线下的方法提供24小时的运营服务。

应持续监控平台系统的性能参数，当性能参数达到告警阈值后须立即分析原因，并采取资源扩容等必要的应对措施。

5. 漏洞和风险管理

应至少每周对平台的操作系统、数据库、WEB应用系统等进行一次全面的漏洞扫描；对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补；短期无法修复的漏洞，要利用现有安全防护设备的策略作为虚拟补丁，进行防护。

应采取技术措施，监测互联网上公开披露的漏洞信息中是否包括平台可能包含的漏洞。

应至少每周对平台的操作系统、数据库、WEB应用系统等的配置参数进行一次全面的基线核查；对基线核查过程中发现的错误的配置参数应及时进行修正；应对修正后的参数进行验证，确认错误参数所造成的隐患已经消除。

除非与平台功能要求有冲突，配置项设置应该遵从产品厂商或专业安全厂商提供的安全配置建议、安全加固指南等文件。

应至少每周对平台的安全防护策略进行一次全面的有效性验证；对于在策略验证中发现的无效策略或防护措施，应尽快进行修复处理。

平台如果运行在虚拟机环境中，应定期对虚拟机镜像进行隐患检查和修复操作。

应至少每年对电子健康卡系统平台进行一次网络安全检测和风险评估，在信息系统或运行环境发生重大变更（包括发现新的威胁和漏洞）时，或者在出现其他可能影响系统安全状态的条件时，重新进行风险评估；对发现的安全问题及时整改，并按照保护工作部门要求报送情况；检测评估内容包括但不限于网络安全制度（国家和行业相关法律法规政策文件及运营者制定的制度）落实情况、组织机构建设情况、人员和经费投入情况、教育培训情况、等保工作落实情况、密评情况、技术防护情况、云服务安全评估情况、风险评估情况、应急演练情况、攻防演练情况等，尤其关注关键设备跨系统、跨区域间的信息流动，及其关键业务流动过程中所经资产的安全防护情况。

6. 网络和系统安全管理

应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户进行控制。

应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容。

应指定专门的部门或人员对电子健康卡系统平台日志、监测和报警数据等进行分析、统计，及时发现可疑行为。

应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库。应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据。应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道。

应保证所有与外部的连接均得到授权和审批，应定期检查违反规定无线上网及其他违反网络安全策略的行为。

7. 配置管理

应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等；并将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。

8. 变更管理

应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施。

应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程。

应建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。

当电子健康卡系统平台运营主体发生合并、分立、解散等情况，应当及时报告保护工作部门，并按照保护工作部门的要求对电子健康卡系统平台进行处置，确保安全。

9. 备份与恢复管理

应识别需要定期备份的重要业务信息、系统数据及软件系统等，并规定备份信息的备份方式、备份频度、存储介质、保存期等。

应根据数据的重要性和数据对系统运行的影响，制定数据的备份程序和恢复程序，并按照程序执行数据的备份和恢复。

10. 应急响应

（1）应急预案管理

应根据《国家网络安全事件应急预案》等要求规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容。

应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容。

应制定密码应用应急策略，做好应急资源准备，当密码应用安全事件发生时，应立即启动应急处置措施，结合实际情况及时处置。

应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练。

应定期对原有的应急预案重新评估，修订完善。

（2）应急演练

应以应急预案为指导方案，定期进行应急演练。

应急演练应安排在平台系统负载的低谷时段，避免因应急演练影响平台的正常业务功能。

（3）应急处置

应及时向安全管理部门报告所发现的安全弱点和可疑事件。

应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训。

对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。

密码应用安全事件发生后，应及时向信息系统主管部门进行报告，事件处置完成后，应及时向信息系统主管部门及归属的密码管理部门报告事件发生情况及处置情况。

11. 外包运维管理

应确保外包运维服务商的选择符合国家的有关规定；应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容；应保证选择的外包运维服务商在技术和管理方面均应具有按照等保要求开展安全运维工作的能力，并将能力要求在签订的协议中明确；应在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对IT基础设施中断服务的应急保障要求等。