国家卫生健康委员会
国家中医药管理局 文件
国家疾病预防控制局

国卫规划发〔2022〕29号

关于印发医疗卫生机构网络安全管理办法的通知

各省、自治区、直辖市及新疆生产建设兵团卫生健康委、中医药局，国家卫生健康委机关各司局、委直属和联系单位、中国老龄协会，国家中医药局、国家疾控局机关各司局、各直属单位：

为指导医疗卫生机构加强网络安全管理，国家卫生健康委、国家中医药局、国家疾控局制定了《医疗卫生机构网络安全管理办法》。现印发给你们，请认真贯彻执行。

国家卫生健康委

国家中医药管理局

2022年8月8日

（信息公开形式：主动公开）

医疗卫生机构网络安全管理办法

第一章　总　则

第一条　为加强医疗卫生机构网络安全管理，进一步促进“互联网＋医疗健康”发展，充分发挥健康医疗大数据作为国家重要基础性战略资源的作用，加强医疗卫生机构网络安全管理，防范网络安全事件发生，根据《基本医疗卫生与健康促进法》《网络安全法》《密码法》《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》《网络安全审查办法》以及网络安全等级保护制度等有关法律法规标准，制定本办法。

第二条　坚持网络安全为人民、网络安全靠人民，坚持网络安全教育、技术、产业融合发展，坚持促进发展和依法管理相统一，坚持安全可控和开放创新并重。

坚持分等级保护、突出重点。重点保障关键信息基础设施、网络安全等级保护第三级（以下简称第三级）及以上网络以及重要数据和个人信息安全。

坚持积极防御、综合防护。充分利用人工智能、大数据分析等技术，强化安全监测、态势感知、通报预警和应急处置等重点工作，落实网络安全保护“实战化、体系化、常态化”和“动态防御、主动防御、纵深防御、精准防护、整体防控、联防联控”的“三化六防”措施。

坚持“管业务就要管安全”“谁主管谁负责、谁运营谁负责、谁

使用谁负责”的原则，落实网络安全责任制，明确各方责任。

第三条 本办法所称的网络是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

本办法所称的数据为网络数据，是指医疗卫生机构通过网络收集、存储、传输、处理和产生的各种电子数据，包括但不限于各类临床、科研、管理等业务数据、医疗设备产生的数据、个人信息以及数据衍生物。

本办法适用于医疗卫生机构运营网络的安全管理。未纳入区域基层卫生信息系统的基层医疗卫生机构参照执行。

第四条 国家卫生健康委、国家中医药局、国家疾控局负责统筹规划、指导、评估、监督医疗卫生机构网络安全工作。县级以上地方卫生健康行政部门（含中医药和疾控部门，下同）负责本行政区域内医疗卫生机构网络安全指导监督工作。

医疗卫生机构对本单位网络安全管理负主体责任，各医疗卫生机构应当与信息化建设参与单位及相关医疗设备生产经营企业书面约定各方的网络安全义务和违约责任。

第二章 网络安全管理

第五条 各医疗卫生机构应成立网络安全和信息化工作领导小组，由单位主要负责人任领导小组组长，每年至少召开一次网络安全办公会，部署安全重点工作，落实《关键信息基础设施安全保

护条例》和网络安全等级保护制度要求。有二级及以上网络的医疗卫生机构应明确负责网络安全管理工作的职能部门，明确承担安全主管、安全管理员等职责的岗位；建立网络安全管理制度体系，加强网络安全防护，强化应急处置，在此基础上对关键信息基础设施实行重点保护，防止网络安全事件发生。

第六条 各医疗卫生机构按照“谁主管谁负责、谁运营谁负责、谁使用谁负责”的原则，在网络建设过程中明确本单位各网络的主管部门、运营部门、信息化部门、使用部门等管理职责，对本单位运营范围内的网络进行等级保护定级、备案、测评、安全建设整改等工作。

（一）对新建网络，应在规划和申报阶段确定网络安全保护等级。各医疗卫生机构应全面梳理本单位各类网络，特别是云计算、物联网、区块链、5G、大数据等新技术应用的基本情况，并根据网络的功能、服务范围、服务对象和处理数据等情况，依据相关标准科学确定网络的安全保护等级，并报上级主管部门审核同意。

（二）新建网络投入使用应依法依规开展等级保护备案工作。第二级以上网络应在网络安全保护等级确定后10个工作日内，由其运营者向公安机关备案，并将备案情况报上级卫生健康行政部门，因网络撤销或变更安全保护等级的，应在10个工作日内向原备案公安机关撤销或变更，同步上报上级卫生健康行政部门。

（三）全面梳理分析网络安全保护需求，按照“一个中心（安全管理中心），三重防护（安全通信网络、安全区域边界、安全计算环

境)”的要求,制定符合网络安全保护等级要求的整体规划和建设方案,加强信息系统自行开发或外包开发过程中的安全管理,认真开展网络安全建设,全面落实安全保护措施。

(四)各医疗卫生机构对已定级备案网络的安全性进行检测评估,第三级或第四级的网络应委托等级保护测评机构,每年至少一次开展网络安全等级测评。第二级的网络应委托等级保护测评机构定期开展网络安全等级测评,其中涉及10万人以上个人信息的网络应至少三年开展一次网络安全等级测评,其他的网络至少五年开展一次网络安全等级测评。新建的网络上线运行前应进行安全性测试。

(五)针对等级测评中发现的问题隐患,各医疗卫生机构要结合外在的威胁风险,按照法律法规、政策和标准要求,制定网络安全整改方案,有针对性地开展整改,及时消除风险隐患,补强管理和技术短板,提升安全防护能力。

第七条 各医疗卫生机构应依托国家网络安全信息通报机制,加强本单位网络安全通报预警力量建设。鼓励三级医院探索态势感知平台建设,及时收集、汇总、分析各方网络安全信息,加强威胁情报工作,组织开展网络安全威胁分析和态势研判,及时通报预警和处置,防止网络被破坏、数据外泄等事件。

第八条 各医疗卫生机构应建立应急处置机制,通过建立完善应急预案、组织应急演练等方式,有效处理网络中断、网络攻击、数据泄露等安全事件,提高应对网络安全事件能力。积极参加网

络安全攻防演练，提升保护和对抗能力。

第九条 各医疗卫生机构在网络运营过程中，应每年开展文档核验、漏洞扫描、渗透测试等多种形式的安全自查，及时发现可能存在的问题和隐患。针对安全自查、监测预警、安全通报等过程中发现的安全隐患应认真开展整改加固，防止网络带病运行，并按要求将安全自查整改情况报上级卫生健康行政部门。自查整改可与等级测评问题整改一并实施。

每年安全自查整改工作包括：

（一）依据上级主管监管机构要求，各医疗卫生机构完成信息资产梳理，摸清本单位网络定级、备案等情况，形成资产清单，组织安全自查。

（二）依据上级主管监管机构要求，各医疗卫生机构依据安全自查结果，对发现的问题和隐患进行整改，形成整改报告向有关主管监管机构报备。

第十条 关键信息基础设施运营者应对安全管理机构负责人和关键岗位人员进行安全背景审查。各医疗卫生机构要加强网络运营相关人员管理，包括本单位内部人员及第三方人员，明确内部人员入职、培训、考核、离岗全流程安全管理，针对第三方应明确人员接触网络时的申请及批准流程，做好实名登记、人员背景审查、保密协议签署等工作，防止因人员资质及违规操作引发的安全风险。

第十一条 加强网络运维管理，制定运维操作规范和工作流

程。加强物理安全防护，完善机房、办公环境及运维现场等安全控制措施，防止非授权访问物理环境造成信息泄露。加强远程运维管理，因业务确需通过互联网远程运维的，应进行评估论证，并采取相应的安全管控措施，防止远程端口暴露引发安全事件。

第十二条 各医疗卫生机构应加强业务连续性管理并持续监测网络运行状态。对于第三级及以上的网络应加强保障关键链路、关键设备冗余备份，有条件的医疗卫生机构应建立应用级容灾备份，防止关键业务中断。

第十三条 应用大数据、人工智能、区块链等新技术开展服务时，上线前应评估新技术的安全风险并进行安全管控，达到应用与安全的平衡。

第十四条 各医疗卫生机构应规范和加强医疗设备数据、个人信息保护和网络安全管理，建立健全医疗设备招标采购、安装调试、运行使用、维护维修、报废处置等相关网络安全管理制度，定期检查或评估医疗设备网络安全，并采取相应的安全管控措施，确保医疗设备网络安全。

第十五条 各医疗卫生机构应按照《密码法》等有关法律法规和密码应用相关标准规范，在网络建设过程中同步规划、同步建设、同步运行密码保护措施，使用符合相关要求的密码产品和服务。

第十六条 各医疗卫生机构应关注整个网络全链条参与者的安全管理，涉及非本单位的第三方时，应对设计、建设、运行、维护

等服务实施安全管理，采购安全的网络产品和服务，防止发生第三方安全事件。

第十七条 各医疗卫生机构应加强废止网络的安全管理，对废止网络的相关设备进行风险评估，及时对其采取封存或销毁措施，确保废止网络中的数据处置安全，防止网络数据泄露。

第三章 数据安全管理

第十八条 各医疗卫生机构应按照有关法律法规的规定，参照国家网络安全标准，履行数据安全保护义务，坚持保障数据安全与发展并重，通过管理和技术手段保障数据安全和数据应用的有效平衡。关键信息基础设施运营者应拟定关键信息基础设施安全保护计划，建立健全数据安全和个人信息保护制度。

第十九条 应建立数据安全管理组织架构，明确业务部门与管理部门在数据安全活动中的主体责任，通过安全责任书等方式，规范本单位数据管理部门、业务部门、信息化部门在数据安全管理全生命周期当中的权责，建立数据安全工作责任制，落实追责追究制度。

第二十条 各医疗卫生机构应每年对数据资产进行全面梳理，在落实网络安全等级保护制度的基础上，依据数据的重要程度以及遭到破坏后的危害程度建立本单位数据分类分级标准。数据分类分级应遵循合法合规原则、可执行原则、时效性原则、自主性原则、差异性原则及客观性原则。

第二十一条 各医疗卫生机构应建立健全数据安全管理制度、操作规程及技术规范，涉及的管理制度每年至少修订一次，建议相关人员每年度签署保密协议。每年对本单位的数据进行数据安全风险评估，及时掌握数据安全状态。加强数据安全教育培训，组织安全意识教育和数据安全管理制度宣传培训。结合本单位实际，建立完善数据使用申请及批准流程，遵循“谁主管、谁审查”、遵循事前申请及批准、事中监管、事后审核原则，严格执行业务管理部门同意、医疗卫生机构领导核准的工作程序，指导数据活动流程合规。

第二十二条 各医疗卫生机构应加强数据收集、存储、传输、处理、使用、交换、销毁全生命周期安全管理工作，数据全生命周期活动应在境内开展，因业务确需向境外提供的，应当按照相关法律法规及有关要求进行安全评估或审核，针对影响或者可能影响国家安全的数据处理活动需提交国家安全审查，防止数据安全事件发生。

（一）各医疗卫生机构应加强数据收集合法性管理，明确业务部门和管理部门在数据收集合法性中的主体责任。采取数据脱敏、数据加密、链路加密等防控措施，防止数据收集过程中数据被泄露。

（二）在数据分类分级的基础上，进一步明确不同安全级别数据的加密传输要求。加强传输过程中的接口安全控制，确保在通过接口传输时的安全性，防止数据被窃取。

（三）各医疗卫生机构应按照有关法规标准，选择合适的数据存储架构和介质在境内存储，并采取备份、加密等措施加强数据的存储安全。涉及到云上存储数据时，应当评估可能带来的安全风险。数据存储周期不应超出数据使用规则确定的保存期限。加强存储过程中访问控制安全、数据副本安全、数据归档安全管控。

（四）各医疗卫生机构应严格规定不同人员的权限，加强数据使用过程中的申请及批准流程管理，确保数据在可控范围内使用，加强日志留存及管理工作，杜绝篡改、删除日志的现象发生，防止数据越权使用。各数据使用部门和数据使用人须严格按照申请所述用途与范围使用数据，对数据的安全负责。未经批准，任何部门和个人不得将未对外公开的信息数据传递至部门外，不得以任何方式将其泄露。

（五）各医疗卫生机构发布、共享数据时应当评估可能带来的安全风险，并采取必要的安全防控措施；涉及数据上报时，应由数据上报提出方负责解读上报要求，确定上报范围和上报规则，确保数据上报安全可控。

（六）各医疗卫生机构开展人脸识别或人脸辨识时，应同时提供非人脸识别的身份识别方式，不得因数据主体不同意收集人脸识别数据而拒绝数据主体使用其基本业务功能，人脸识别数据不得用于除身份识别之外的其他目的，包括但不限于评估或预测数据主体工作表现、经济状况、健康状况、偏好、兴趣等。各医疗卫生机构应采取安全措施存储和传输人脸识别数据，包括但不限于加

密存储和传输人脸识别数据，采用物理或逻辑隔离方式分别存储人脸识别和个人身份信息等。

（七）数据销毁时应采用确保数据无法还原的销毁方式，重点关注数据残留风险及数据备份风险。

第四章　监督管理

第二十三条　各医疗卫生机构应积极配合有关主管监管机构监督管理，接受网络安全管理日常检查，做好网络安全防护等工作。

第二十四条　各医疗卫生机构应及时整改有关主管监管机构检查过程中发现的漏洞和隐患等问题，杜绝重大网络安全事件发生。

第二十五条　发生个人信息和数据泄露、毁损、丢失等安全事件和网络系统遭攻击、入侵、控制等网络安全事件，或者发现网络存在漏洞隐患、网络安全风险明显增大时，各医疗卫生机构应当立即启动应急预案，采取必要的补救和处置措施，及时以电话、短信、邮件或信函等多种方式告知相关主体，并按照要求向有关主管监管部门报告。

第二十六条　各级卫生健康行政部门应建立网络安全事件通报工作机制，及时通报网络安全事件。

第二十七条　发生网络安全事件时，各医疗卫生机构应及时向卫生健康行政部门、公安机关报告，做好现场保护、留存相关记

录，为公安机关等监管部门依法维护国家安全和开展侦查调查等活动提供技术支持和协助。

第五章　管理保障

第二十八条　各医疗卫生机构应高度重视网络安全管理工作，将其列入重要议事日程，加强统筹领导和规划设计，依法依规落实人员、经费投入、安全保护措施建设等重大问题，保证信息系统建设时安全保护措施同步规划、同步建设和同步使用。

第二十九条　各医疗卫生机构应加强网络安全业务交流，严格执行网络安全继续教育制度，鼓励管理岗位和技术岗位持证上岗。通过组织开展学术交流及比武竞赛的方式，发现选拔网络安全人才，建立人才库，建立健全人才发现、培养、选拔和使用机制，为做好网络安全工作提供人才保障。

第三十条　各医疗卫生机构应保障开展网络安全等级测评、风险评估、攻防演练竞赛、安全建设整改、安全保护平台建设、密码保障系统建设、运维、教育培训等经费投入。新建信息化项目的网络安全预算不低于项目总预算的5%。

第三十一条　各医疗卫生机构应进一步完善网络安全考核评价制度，明确考核指标，组织开展考核。鼓励有条件的医疗卫生机构将考核与绩效挂钩。

第六章　附　则

第三十二条　违反本办法规定，发生个人信息和数据泄露，或者出现重大网络安全事件的，按《网络安全法》《密码法》《基本医疗卫生与健康促进法》《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》以及网络安全等级保护制度等法律法规处理。

第三十三条　涉及国家秘密的网络，按照国家有关规定执行。

第三十四条　本办法自印发之日起实施。

国家卫生健康委办公厅　　2022年8月16日印发

校对：曾红涛