国家医疗保障局关于印发加强网络安全和数据保护工作指导意见的通知

医保发〔2021〕23号

各省、自治区、直辖市及新疆生产建设兵团医疗保障局、局内各单位：

《国家医疗保障局关于加强网络安全和数据保护工作的指导意见》已经第44次局长办公会审议通过，现印发给你们，请遵照执行。

附件：国家医疗保障局关于加强网络安全和数据保护工作的指导意见

国家医疗保障局

2021年4月6日

国家医疗保障局关于加强网络安全和数据保护工作的指导意见

医疗保障信息化是医疗保障事业高质量发展的基础，是医保治理体系和治理能力现代化的重要支撑。为全面落实习近平总书记关于网络强国战略、大数据战略、数字经济的重要指示批示精神，以及党中央关于网络安全工作的总体部署，扎实推进医疗保障信息平台建设及运营维护，防范化解医疗保障系统数据安全风险，促进数据合理安全开发利用，现就加强医疗保障网络安全和数据保护工作，提出以下指导意见。

一、总体要求

（一）指导思想

坚持以习近平新时代中国特色社会主义思想为指导，全面贯彻党的十九大和十九届二中、三中、四中、五中全会精神，坚持总体国家安全观，深入实施网络强国和大数据战略，以医保系统网络安全为基础，以智慧医保和安全医保建设为目标，以医保信息安全技术为支撑，以制度建设和人才队伍建设为保障，筑牢安全防线，促进数据安全应用，更好助力医保治理体系和治理能力现代化，推动医保事业高质量发展。

（二）基本原则

坚持安全为本，促进发展。统筹网络安全保障和数据安全保护，夯实医疗保障信息化发展的安全底线，稳步推动医保大数据建设，为智慧医保建设、合法合规数据信息共享、多层次医疗保障体系建设提供有力支撑。

坚持健全制度，强化技术。制定实施网络安全管理和数据安全保护的系列制度，建立有效工作机制，广泛运用先进的网络安全和数据安全保护技术，建立健全数据安全治理体系，提高数据安全保障能力。

坚持强化基础，提升能力。把网络基础设施建设放在重要位置，加快提升医疗保障系统网络安全管理能力、数据安全保护能力、数据共享服务能力，加强人才队伍建设，筑牢安全发展基础。

坚持明晰责任，闭环管理。坚持“谁主管、谁负责，谁使用、谁负责”原则，落实网络安全责任制，落实数据主管单位、数据使用单位责任，建立健全安全审查审批和权限管理机制，实现数据全流程全生命周期管理。

（三）主要目标

到 2022 年，基本建成基础强、技术优、制度全、责任明、管理严的医疗保障网络安全和数据安全保护工作体制机制。到“十四五”期末，医疗保障系统网络安全和数据安全保护制度体系更加健全，智慧医保和安全医保建设达到新水平。

——网络安全水平显著提升。主体责任明晰，监督管理机制完善，基础设施完备，网络安全技术能力、态势感知、预警能力、突发网络安全事件应急响应能力显著提升，网络安全有效保障。

——数据安全管理有效实施。数据安全审批制度全面建立，分级分类管理及重要数据保护目录全面落实，数据实现全生命周期安全管理，数据安全评估机制日益完善。

——数据共享使用安全有序。数据共享使用流程明晰、机制健全，医疗保障数字化、智能化水平显著提升。

二、加强网络安全管理

（一）落实网络安全主体责任

建立健全网络安全责任制。各级医保部门是本级网络安全的责任主体，各级医保部门主要负责人是第一责任人。各级医保部门要组建网络安全和信息化领导小组，落实网络安全主体责任，明确信息技术保障和意识形态工作责任边界，强化行政部门网络安全管理责任和担当，健全考核机制，严格责任追究，确保网络安全责任全覆盖。

（二）完善网络安全监督管理机制

各级医保部门要强化日常工作中网络安全“红线”意识和底线思维，建立多环节、多层次、全方位的网络安全监督管理机制。定期对信息系统运行的相关软硬件开展安全防护检查。对涉及关键网络岗位和重要数据岗位的从业人员实施严格的背景审查。全面梳理网络、系统和关键设备的网络安全责任部门和责任人。

（三）加强关键信息基础设施安全保护

全面推进网络安全等级保护工作。根据行业规范合理定级备案，在系统规划、设计阶段同步确定安全保护等级，按照国家和行业标准进行等级测评。切实落实关键信息基础设施重点保护要求，加强关键信息基础设施网络安全监测预警体系建设，提升关键信息基础设施应急响应和恢复能力。按照“安全分区、网络专用、横向隔离、纵向认证”的原则，进一步完善网络结构安全、本体安全和基础设施安全，逐步推广安全免疫。加强内外网安全隔离，严禁医保专网接入互联网。

（四）强化网络安全技术防护能力

建立并完善入侵检测与防御、防病毒、防拒绝服务攻击、防信息泄露、异常流量监测、网页防篡改、域名安全、漏洞扫描、集中账号管理、数据加密、安全审计等网络安全防护技术手段。积极研究利用云计算、大数据等技术提高网络安全监测预警能力。加强网站安全防护和日常办公、维护终端的安全管理。完善域名系统安全防护措施，做好网络和业务系统上线前的风险评估。

（五）提高网络安全态势感知、预警和协同能力

加强网络安全和数据保护“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，推进

全国医疗保障信息系统网络安全和数据保护态势感知、预警能力建设。加强网络安全和数据保护信息的汇集、研判，建立健全网络安全和数据保护信息共享和通报机制，健全完善上下协同的通报预警机制。

（六）提升突发网络安全事件应急响应能力

严格落实突发网络安全事件报告制度。制定和完善本单位网络安全应急预案。健全大规模拒绝服务攻击、高级可持续性威胁攻击、大规模公民个人信息泄露等突发网络安全事件的应急协同配合机制，加强应急预案演练，定期评估和修订应急预案，提高科学性、实用性、可操作性。建立重大活动期间网络安全保障机制，强化对网络安全突发事件的统一指挥和协调，确保全国医疗保障信息系统的运行安全、数据安全和网络安全，最大程度地预防和减少网络安全事件造成的损害。

三、加强数据安全保护

（一）实施数据全生命周期安全管理

依法依规对数据的产生、传输、存储、使用、共享、销毁等实行全生命周期安全管理，提高数据安全防护能力和个人隐私保护力度。强化个人隐私保护，采用适当的安全控制措施，确保数据的产生、采集和汇集过程合规、安全。个人信息的采集，坚持法定授权原则，法定授权外个人信息采集事项须先获得自然人或者其监护人同意。处理个人信息应当遵循合法、正当、必要原则，不得过度使用。采用适当的系统架构、技术手段对数据传输和数据存储进行安全加固，确保数据安全和高效可用。建立数据清除和销毁机制，防止因存储介质上数据内容的恶意恢复而导致的数据泄露风险。加强数据迁移销毁流程安全管理，全力确保平台迁移中的数据安全。

（二）实施分级分类管理

根据本单位本系统数据安全保护的实际需要，结合医疗保障数据特点，制定统一的分级分类管理制度，按照数据分级分类保护标准、规则，对数据划分安全等级，实行分级分类管理。地方医保部门要落实分级分类规则标准，参照《国家医疗保障局数据安全管理办法》制定本地的数据安全管理办法。

（三）加强重要数据和敏感字段保护

制定重要数据保护目录，对列入目录的数据进行重点保护，涉及国家秘密、工作秘密的数据应严格保密，不予共享及公开。建立敏感数据字段库，包含但不限于个人隐私数据、参保单位隐私数据、协议机构隐私数据、药品诊疗目录项目隐私数据等。

（四）强化数据安全审批管理

严格执行数据处理和使用审批流程，按照“知所必须，最小授权”的原则划分数据访问权限，实施脱敏、日志记录等控制措施，防范数据丢失、泄露、未授权访问等安全风险。

加强对数据共享(含交换、导出、开放)环节的安全管控，防止不经审批、不受控制的数据共享行为。

（五）落实数据安全权限

明确各级权限，分离信息系统运维权限和经办业务角色，对不同角色设置不同权限。根据经办业务人员职责区分设置业务操作和数据查询范围。按照网络安全等级保护 2.0 制度要求，结合实际设置安全保密管理员、安全审计员和系统管理员等岗位。加强信息系统运维人员和经办业务人员权限管理，落实岗位安全职责。

（六）推动数据安全共享和使用

在保障数据安全的前提下，稳妥推动数据资源开发利用，发挥数据生产要素作用，保障数据依法依规有序共享。建立先试点、后推广机制，强化医疗保障大数据运用，更好地服务医保政策制定和医保精细化管理，推动多层次医疗保障体系建设。对于敏感数据需要落地到外部的业务场景，应做好脱敏处理，制定统一数据出口和统一销毁要求，建立严格的审批流程和数据交付流程。

（七）建立健全数据安全风险评估机制

定期评估安全系统软硬件运行状况、制度执行情况、数据复制情况、告警或故障设备的数据保护状况、权限的审批收回情况、密码强度、外包服务中的数据保护管理情况、研发测试环境数据保护情况，对发现的问题及时整改。

四、保障措施

（一）加强组织领导

各级医保部门要充分认识加强网络安全和数据保护工作的重要性，加强组织领导，做好部门协调，层层落实责任，确保相关部署落到实处。要建立相应工作机制，夯实工作力量，科学合理制定工作推进时间安排，周密组织实施网络安全管理和数据保护工作，切实提高医疗保障网络安全和数据保护工作水平。

（二）加强人才队伍建设

加大网络安全和数据保护人才培养投入，加强从业人员技能培训，形成培养、选拔、吸引和使用网络安全和数据保护人才的良性机制。建立各级医保部门网络和数据安全专家库。

（三）加强资金投入

各级医保部门应加强统筹规划，做好网络安全和数据保护体系顶层设计，制定工作计划。按照总体进度安排和工作目标，将网络安全和数据保护建设、运行维护经费纳入信息化建设项目投入，加强资金保障和使用监管，确保网络安全和数据保护工作的资金投入。

（四）加强法律法规宣传

积极宣传网络安全法律法规，定期组织网络安全和数据保护培训交流，对产品和服务供应商加强网络安全和数据保护教育，提升全员网络安全和数据保护意识，为网络安全和数据保护治理营造良好氛围。

（五）加强督导检查

要将网络安全与数据保护工作推进情况纳入本单位工作考核范畴，建立督查情况通报制度，对工作不力的要及时督查整改，确保网络安全和数据保护工作万

无一失。对工作中出现问题造成不良后果的单位及人员要通报批评，造成严重后果的要依纪依法问责处理。