国家卫生健康委
公安部
国家互联网信息办公室 文件
国家中医药管理局
国家疾病预防控制局

国卫规划发〔2026〕6号

关于印发医疗卫生机构数据安全和个人信息保护管理办法（试行）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、公安厅（局）、互联网信息办公室、中医药局、疾控局，委（部、办、局）机关各司局、各直属和联系单位：

为指导医疗卫生机构加强数据安全和个人信息保护管理，国家卫生健康委、公安部、国家互联网信息办公室、国家中医药局、国家疾控局制定了《医疗卫生机构数据安全和个人信息保护管理办

法（试行）》。现印发给你们，请认真贯彻执行。

国家卫生健康委　　公安部

国家互联网信息办公室　　国家中医药局

国家疾病预防控制局

2026年2月12日

（信息公开形式：依申请公开）

医疗卫生机构数据安全和个人信息保护管理办法(试行)

第一章　总　则

第一条　为了规范医疗卫生机构数据安全和个人信息保护管理,促进医疗卫生机构数据开发和个人信息合理利用,保护个人、组织的合法权益,统筹发展和安全,根据《中华人民共和国网络安全法》《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》《中华人民共和国基本医疗卫生与健康促进法》《网络数据安全管理条例》等法律、行政法规,制定本办法。

第二条　本办法适用于医疗卫生机构的数据安全和个人信息保护管理。

本办法所称的数据,是指任何以电子或者其他方式对信息的记录。

本办法所称的医疗卫生机构数据,是指医疗卫生机构收集和产生的各种数据,包括但不限于各类临床、科研、管理等业务数据与医疗设备产生的数据。

本办法所称的数据处理活动,包括数据的收集、存储、使用、加工、传输、提供、公开等。

个人信息是特别重要的一种数据，当达到一定精度、规模时，个人信息要按照数据分类分级管理要求，纳入国家重要数据目录进行重点保护。

第三条 在国家数据安全工作协调机制的统一部署下，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、监督医疗卫生机构数据安全和个人信息保护管理工作。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数据安全和个人信息保护管理工作。医疗卫生机构按照属地管理的原则，接受卫生健康行政部门监管。

第四条 医疗卫生机构对本单位医疗卫生机构数据安全和个人信息保护管理负主体责任，县级以上医疗卫生机构应当成立网络安全和信息化工作领导小组，由单位主要负责人担任组长，每年至少召开一次医疗卫生机构数据安全和个人信息保护会议，部署数据安全和个人信息保护工作，研究制定相关制度规范。

医疗卫生机构主要负责人是本单位数据安全和个人信息保护管理第一责任人，分管负责人是直接责任人。按照“管业务必须管安全”“谁主管谁负责、谁运营谁负责、谁使用谁负责”的原则，明确本单位业务部门与信息化部门的职责，加强医疗卫生机构数据安全和个人信息保护管理。

第二章　数据分类分级保护

第五条　依据有关法律和卫生健康行业数据分类分级有关要求，医疗卫生机构数据分为核心数据、重要数据和一般数据，落实分类分级保护制度。不同类别、级别数据同时被处理且难以分别采取保护措施的，按照其中级别最高的要求实施保护。

第六条　省级卫生健康行政部门按照卫生健康行业数据分类分级有关要求组织开展省域内医疗卫生机构数据的分类分级工作，提出重要数据具体目录和核心数据目录建议并报国家卫生健康委（中医领域报送国家中医药局、疾控领域报送国家疾控局），目录发生变化的，应当及时更新并上报。各级卫生健康行政部门确认为重要数据的，应当及时告知医疗卫生机构。

医疗卫生机构应当定期梳理医疗卫生机构数据，确定医疗卫生机构数据类别，识别重要数据，并向属地卫生健康行政部门报送，上报内容包括但不限于医疗卫生机构数据来源、类别、级别、规模、处理目的和方式、责任主体、跨境传输、安全保护措施等基本情况，不包括医疗卫生机构数据内容本身。

第七条　医疗卫生机构数据级别确定后，出现下列情形之一的，应对医疗卫生机构数据级别及时变更：

（一）医疗卫生机构数据内容发生较大变化。

（二）医疗卫生机构数据内容未发生变化，但医疗卫生机构数

据规模、医疗卫生机构数据时效性、医疗卫生机构数据应用场景、医疗卫生机构数据加工处理方式等发生较大变化。

（三）需要对医疗卫生机构数据级别进行变更的其他情形。

第八条 医疗卫生机构数据经过脱敏、标签、统计、汇聚融合等加工活动而产生的衍生数据，应在原始数据定级的基础上，重新评估确定数据级别。

第三章 数据全生命周期安全管理

第九条 医疗卫生机构开展医疗卫生机构数据和个人信息处理活动，应当遵守法律法规规定，履行相应数据安全保护义务，坚持保障数据安全与发展并重，通过管理和技术手段保障医疗卫生机构数据安全和医疗卫生机构数据应用的有效平衡，通过开展包括但不限于以下工作，确保医疗卫生机构数据持续处于有效保护和合法合规利用的状态，防止未经授权的访问以及个人信息泄露、篡改、丢失：

（一）强化制度保障。建立医疗卫生机构数据安全管理制度、操作规程及技术规范，针对不同类别和级别的医疗卫生机构数据，明确收集、存储、使用、加工、传输、提供、公开等环节的具体保护要求。

（二）强化人员保障。加强医疗卫生机构数据安全管理人员队

伍建设，定期开展医疗卫生机构数据安全教育和培训，提高全员数据安全、个人信息保护意识和水平。

（三）强化管理保障。严格医疗卫生机构数据和个人信息处理活动的日常管理，明确处理的操作权限。自行或委托第三方评估机构定期对本单位的医疗卫生机构数据进行安全风险评估，及时掌握数据安全状态，及时整改风险问题，消除隐患，并向属地卫生健康行政部门报送风险评估报告。

（四）强化技术保障。在医疗卫生机构数据的收集、存储、使用、加工、传输、提供、公开、删除等环节，针对不同场景综合运用加密、鉴权、认证、脱敏、去标识化、数字水印、校验、审计等技术手段进行安全保护。

（五）强化应急保障。根据工作实际与应对医疗卫生机构数据安全事件的需要，应制定完善应急预案，并定期开展演练。

（六）法律、行政法规等规定的其他措施。

第十条 处理重要数据的医疗卫生机构，应当明确医疗卫生机构数据安全负责人和管理机构，落实医疗卫生机构数据安全保护责任，每年度对其医疗卫生机构数据处理活动开展风险评估，并向省级及以上卫生健康行政部门报送风险评估报告，卫生健康行政部门应当及时通报同级网信部门、公安机关。医疗卫生机构提供、委托处理、共同处理重要数据前应当进行风险评估，属于履行

法定职责或者法定义务的除外。

医疗卫生机构向其他医疗卫生机构数据处理者提供、委托处理重要数据的，应当通过合同等方式与接收方约定处理目的、方式、范围以及安全保护义务等，并对医疗卫生机构数据接收方履行义务的情况进行监督。

第十一条 医疗卫生机构在存储处理重要数据时要落实三级及以上网络安全等级保护要求。存储处理核心数据的，涉及关键信息基础设施的，要在网络安全等级保护制度的基础上，落实关键信息基础设施安全保护要求，不涉及关键信息基础设施的，应落实四级网络安全等级保护要求。医疗卫生机构数据内容发生较大变化，需要变更医疗卫生机构数据级别的，应根据情况及时进行网络安全等级保护重新定级备案。法律法规和国家有关规定要求使用商用密码进行保护的，应当遵守商用密码保护有关规定。

进行核心数据跨不同法人主体提供、转移、共享等活动时，应采取必要的安全保护措施，并告知数据接收方按照对应级别进行分类分级保护。自当年度1月1日起可能累计达到上一年度末该项核心数据静态总量30%及以上的，应经国家卫生健康委报有关部门组织风险评估。涉及国家机关依法履职、国家机关或企事业单位内部流动的除外。

医疗卫生机构在处理核心数据时，在重要数据保护要求的基

础上：

（一）优先使用商用密码进行保护；

（二）优先使用安全可信的产品和服务；

（三）优先使用第三方评估机构开展风险评估；

（四）涉及核心数据安全事件处置、溯源的相关日志留存时间不少于三年；

（五）对相关关键岗位人员、涉核心数据信息系统建设和运维单位等，提交公安机关、国家安全机关进行国家安全背景审查。

第十二条 支持医疗卫生机构在确保医疗卫生机构数据安全的前提下，依法依规加强医疗卫生机构数据共享。医疗卫生机构应当加强对医疗卫生机构数据共享、调用的安全管理，采取技术措施定期监测医疗卫生机构数据共享调用等情况，对医疗卫生机构数据查询、下载、修改、删除等操作日志开展审计分析，及时发现违规或异常行为，采取相应处置措施，并配备认证鉴权、威胁告警等安全保护措施。

第十三条 支持医疗卫生机构在确保医疗卫生机构数据和个人信息安全的前提下，依法依规加强数据要素开发利用工作。

医疗卫生机构应当建立完善医疗卫生机构数据使用申请及批准流程，遵循“谁主管、谁审查”，坚持事前申请批准、事中监管、事后审核的原则，严格执行业务管理部门同意、医疗卫生机构领导核

准、信息技术部门支撑执行的工作程序，如涉及对外提供医疗卫生机构数据的，需按相关要求报审，确保医疗卫生机构数据活动流程合法合规。医疗卫生机构应当对医疗卫生机构数据接收方履行安全管理责任进行监督。

鼓励医疗卫生机构通过“原始数据不出域，数据可用不可见，数据可控可计量”等方式，促进医疗卫生机构数据依法合理有效利用。

第十四条 医疗卫生机构依据国家关于公共数据资源开发利用的有关规定，按照公共数据资源授权运营实施规范，探索建立数据分类分级授权运营机制，将授权运营纳入医疗卫生机构领导班子集体决策范围，明确授权条件、运营模式、运营期限、退出机制和安全管理责任，授权符合条件的运营机构开展公共数据资源开发、产品经营和技术服务。

第十五条 卫生健康行政部门等国家机关为履行法定职责需要收集、使用数据，应当在其履行法定职责的范围内依照法律、行政法规规定的条件和程序进行。法律、行政法规和国家有关规定明确医疗卫生机构可以拒绝其他行政部门重复采集医疗卫生机构数据的，医疗卫生机构可以拒绝相关组织或个人收集超出履行法定职责所必需的范围和限度的医疗卫生机构数据。

各级卫生健康行政部门应当按照《中华人民共和国数据安全

法》等法律、行政法规和国家有关规定，切实履行行业监管职责，加强向医疗卫生机构采集数据的归口管理，建立健全医疗卫生机构数据共享共用机制，加强部门间数据共享，各级全民健康信息平台和各级传染病监测预警与应急指挥平台已经采集的医疗卫生机构数据，原则上应通过跨部门共享交换实现。

医疗卫生机构应当及时将对外提供医疗卫生机构数据的情况报告属地卫生健康行政部门。属地卫生健康行政部门应当依法依规加强医疗卫生机构数据报送管理，重点管理重复采集医疗卫生机构数据、超范围采集医疗卫生机构数据等违反有关规定的情形。

第十六条 医疗卫生机构委托他人处理或与他人共同处理医疗卫生机构数据的，数据安全责任不因委托而改变。医疗卫生机构应当经过严格的审批程序，明确受托方的数据处理权限和保护责任，并监督受托方履行数据安全保护义务。

涉及使用云计算服务处理医疗卫生机构数据的，应当选择通过云计算服务安全评估的云计算服务，并同时遵守本办法有关要求。

卫生健康行政部门原则上不得委托学会、协会面向医疗卫生机构采集数据，确有必要的，应当经过卫生健康行政部门数据管理机构的统筹论证，并报同级卫生健康行政部门网络安全和信息化工作领导小组审核。

第十七条 医疗卫生机构应当与参与其信息化建设运行维护的相关单位及涉及医疗卫生机构数据存储的相关医疗设备生产经营企业书面约定各方义务和责任，落实责任追究制度。

第十八条 医疗卫生机构应当按照业务工作需要和最小授权原则，依据岗位职责设定医疗卫生机构数据处理权限，控制医疗卫生机构数据接触范围，人员变动时应当及时调整权限。

第十九条 重要数据处理活动应当记录维护数据安全所需的日志，涉及安全事件处置、溯源的，相关日志留存时间应当不少于一年；涉及向他人提供、委托处理、共同处理重要数据的，相关日志留存时间应当不少于三年。

第二十条 医疗卫生机构在使用人工智能等新技术处理医疗卫生机构数据时，应当评估使用新技术带来的安全风险，采取必要的技术措施，加强医疗卫生机构数据安全防护。

第二十一条 医疗卫生机构因合并、分立、解散、被宣告破产等原因需要转移、销毁医疗卫生机构数据的，应当采取必要的安全保护措施，并事前向属地卫生健康行政部门报告医疗卫生机构数据处置方案。引起医疗卫生机构数据目录发生变化的，应当及时报告属地卫生健康行政部门。

第二十二条 医疗卫生机构应当加强对医疗卫生机构数据全生命周期的管理，医疗卫生机构及其人员不得有以下行为：

（一）不得违法采集医疗卫生机构数据。医疗卫生机构应当加强医疗卫生机构数据收集的合法性管理，明确业务部门和管理部门在医疗卫生机构数据收集合法性中的主体责任，不得超范围采集医疗卫生机构数据，不得窃取或者以其他非法方式采集医疗卫生机构数据。

（二）不得违法存储医疗卫生机构数据。医疗卫生机构在我国境内收集和产生的重要数据，应当在境内存储，并采取备份、加密等措施加强医疗卫生机构数据的存储安全。

（三）不得违法进行医疗卫生机构数据传输。医疗卫生机构应当在数据分类分级的基础上，进一步明确不同安全级别医疗卫生机构数据的加密传输要求，不得通过邮箱、网盘、社交软件等传输核心数据、重要数据和敏感数据。加强传输过程中的接口安全控制，采取数据脱敏、数据加密、链路加密等防控措施，确保在通过接口传输时的安全性，防止医疗卫生机构数据被窃取。

（四）不得违法向境外提供医疗卫生机构数据。医疗卫生机构采集的医疗卫生机构数据确需向境外提供，具有国家互联网信息办公室《促进和规范数据跨境流动规定》第七条规定情形之一的，医疗卫生机构应当先行开展自评估工作，经本单位网络安全和信息化工作领导小组或领导班子同意并报属地卫生健康行政部门审核通过后，由省级网信部门向国家网信部门申报医疗卫生机构数

据出境安全评估。医疗卫生机构在学术合作活动中收集和产生的医疗卫生机构数据向境外提供，不包含个人信息、敏感数据或重要数据的，免予申报医疗卫生机构数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证。

（五）不得越权使用医疗卫生机构数据。医疗卫生机构应当严格规定不同人员的权限，加强医疗卫生机构数据使用过程中的申请及批准流程管理，加强日志留存及管理工作，不得篡改、删除日志，确保医疗卫生机构数据在可控范围内使用，防止医疗卫生机构数据越权使用。医疗卫生机构数据使用部门和医疗卫生机构数据使用者应当严格按照申请所述用途与范围使用医疗卫生机构数据，对医疗卫生机构数据的安全负责。非本医疗卫生机构人员在无监管情况下，不得对信息系统或医疗设备进行远程运维。

（六）不得未经授权处理医疗卫生机构数据。未经医疗卫生机构授权，医疗卫生机构信息系统建设运维人员不得处理医疗卫生机构数据；建设运维期间，收集产生的医疗卫生机构数据未经授权不得用于其他用途，服务完成后按照约定对医疗卫生机构数据予以返还或销毁；信息系统建设运维项目的承担单位，未经批准不得转包、分包。

（七）不得未经批准提供医疗卫生机构数据。未经医疗卫生机构网络安全和信息化工作领导小组或领导班子批准，任何部门和

个人不得将未对外公开的信息和医疗卫生机构数据传递至医疗卫生机构之外，不得以任何方式将其泄露。

（八）不得随意公开医疗卫生机构数据。医疗卫生机构在对医疗卫生机构数据公开前，应当分析研判可能对国家安全、经济社会安全、公共利益、个人信息安全及医疗卫生机构运行产生的影响，存在重大影响的不得公开。

（九）不得未经销毁医疗卫生机构数据报废设备或变更用途。医疗卫生机构在设备报废或变更用途前，应当按照电子产品信息清除技术要求对医疗卫生机构数据进行彻底清除处理，不得未经处置直接报废或转移他用。

（十）不得隐瞒医疗卫生机构数据安全事件。医疗卫生机构发生医疗卫生机构数据安全事件时，应当立即启动应急预案，采取措施防止危害扩大，消除安全隐患，并按照规定向属地卫生健康行政部门等有关主管部门报告。

第四章　数据安全监测预警和应急处置

第二十三条　国家卫生健康委建立健全医疗卫生机构数据安全风险监测预警机制，组织制定医疗卫生机构数据安全监测预警标准规范，统筹运用医疗卫生机构数据安全监测预警技术手段，具备监测、预警、处置、溯源等能力，与相关部门加强信息共享。

地方卫生健康行政部门建立健全本地区医疗卫生机构数据安全风险监测预警机制，组织开展医疗卫生机构数据安全风险监测，按照有关规定及时发布预警信息，指导医疗卫生机构及时采取应对措施。

医疗卫生机构应当建立医疗卫生机构数据安全风险监测预警与应急处置机制，及时通过国家信息安全漏洞共享平台等渠道获取信息系统应用漏洞，通过升级补丁、配置更新、系统加固等技术措施，防范医疗卫生机构数据被篡改、泄露、丢失等安全风险。

第二十四条 国家卫生健康委建立健全医疗卫生机构数据安全风险信息上报和共享机制，统一汇集、分析、研判、通报医疗卫生机构数据安全风险隐患，鼓励行业组织、安全服务机构、科研院所等开展医疗卫生机构数据安全风险信息上报和共享。

地方卫生健康行政部门及时汇总分析本地区医疗卫生机构数据安全风险隐患，将可能造成重要数据或核心数据安全事件的风险隐患上报国家卫生健康委（中医领域报送国家中医药局、疾控领域报送国家疾控局）。

医疗卫生机构应当及时将可能造成重要数据或核心数据安全事件的风险隐患向属地卫生健康行政部门报告。

第二十五条 国家卫生健康委制定卫生健康行业数据安全事件应急预案并开展应急演练，指导涉及重要数据和核心数据的安

全事件应急处置工作。

地方卫生健康行政部门分别组织开展本地区医疗卫生机构数据安全事件应急处置工作。涉及重要数据和核心数据的安全事件，应当立即上报国家卫生健康委，并及时报告事件发展和处置情况。

医疗卫生机构应当制定医疗卫生机构数据安全事件应急预案，并定期组织演练。发生医疗卫生机构数据安全事件后，应当按照应急预案，及时开展应急处置，涉及重要数据和核心数据的安全事件，及时向属地卫生健康行政部门报告，安全事件处置完成后应当及时形成总结报告。发生医疗卫生机构数据安全事件时，应当及时告知用户，并采取避免、减轻危害的处置措施，同时向属地卫生健康行政部门报告。

第五章　个人信息保护

第二十六条　医疗卫生机构应当按照《个人信息保护合规审计管理办法》要求，自行或者委托专业机构定期开展个人信息保护合规审计工作。

第二十七条　医疗卫生机构委托处理个人信息时，应当事前进行个人信息保护影响评估并与受托方签订委托协议和保密协议，明确委托处理范围、目的、期限、处理方式、个人信息种类、保护

措施以及双方的权利和义务，并监督协议执行情况。受托方应当按照约定处理个人信息，不得超出约定的处理目的、处理方式等处理个人信息。委托合同不生效、无效、被撤销或者终止的，受托方应当将个人信息返还医疗卫生机构或者予以删除，不得保留。未经个人信息处理者同意，受托方不得委托他人处理个人信息。受托方应当对从业人员开展岗前培训和离职审查。

第二十八条 医疗卫生机构在使用人工智能等新技术过程中，涉及患者病历等个人信息的，必须确保个人信息安全。

第二十九条 医疗卫生机构应当加强对个人信息的保护，医疗卫生机构及其人员不得有以下行为：

（一）不得违法处理个人信息。医疗卫生机构及其人员不得违法收集、存储、使用、加工、传输、提供、公开、删除个人信息，不得非法买卖、提供或者公开传播个人信息，不得从事危害国家安全、公共利益的个人信息处理活动。

（二）不得违法收集个人信息。医疗卫生机构收集个人信息应当遵循合法、正当、必要和诚信原则，不得通过误导、欺诈、胁迫等方式收集个人信息。

（三）不得超范围收集个人信息。医疗卫生机构收集个人信息应当具有明确、合理的目的，应当限于实现处理目的的最小范围，不得过度收集个人信息。

（四）不得超授权调阅个人信息。医疗卫生机构应当采取有效措施和技术手段，严格身份认证，防范患者个人信息被无关人员违法查询或调取，应当制定授权规则，通过场景管理和人员管理结合的方式，明确医疗、教学、科研和公共卫生紧急情况等合法调阅情形，不得违法调阅，重点加强孕产妇、新生儿、艾滋病人、精神障碍患者、逝者及遗属、公众人物等特殊人群个人信息管理。区分不同岗位和人员，实行动态授权管理，及时回收离职离岗、转岗人员权限。推广使用授权管理、日志存档、数字水印等技术进行调阅权限管理，确保个人信息操作痕迹、标记操作时间和操作人员信息可查询、可追溯。

（五）不得违法提供个人信息。未经本人或者其监护人同意，医疗卫生机构及其人员不得超出工作需要提供个人的姓名、出生日期、身份证号码、生物识别信息、住址、电话号码、行踪轨迹等个人信息，为应对突发公共卫生事件或者紧急情况下为保护自然人的生命健康所必需等法律、行政法规另有规定的除外。因国家机关履行法定职责提供的，不得超出履行法定职责所必需的范围和限度。

（六）不得违法公开个人信息。医疗卫生机构不得在电子屏等公共区域，显示患者的个人姓名、身份证号码、电话号码等个人信息，确因业务需要的，应当脱敏显示。未经本人同意，不得在新闻

报道、公开讲座、社交媒体、学术论文、科学研究等场景中公开患者个人信息。不得通过通讯软件、社交媒体等方式传输患者个人信息，不得通过拍照、截图等方式公开患者个人信息。

（七）不得违法向境外提供个人信息。医疗卫生机构因业务等需要，确需向境外提供个人信息的，应当符合《中华人民共和国个人信息保护法》第三十八条规定的条件，并向个人告知境外接收方的名称或者姓名、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使有关权利的方式和程序等事项，取得个人的单独同意。

（八）不得滥用人脸识别信息。应用人脸识别技术验证个人身份、辨识特定个人的，鼓励优先使用国家人口基础信息库、国家网络身份认证公共服务等渠道实施。实现相同目的或者达到同等业务要求，存在其他非人脸识别技术方式的，医疗卫生机构不得将人脸识别技术作为唯一验证方式。个人不同意通过人脸信息进行身份验证的，医疗卫生机构应当提供其他合理、便捷的方式。除法律法规另有规定或者取得个人单独同意外，人脸信息应当存储于人脸识别设备内，不得通过互联网对外传输。

第六章　监督管理

第三十条　各级卫生健康行政部门发现医疗卫生机构数据处

理活动存在较大安全风险或者发生数据安全事件的，应当督促指导医疗卫生机构及时处置并整改。

医疗卫生机构对卫生健康行政部门通报指出的安全漏洞隐患，应当及时开展安全整改加固，堵塞漏洞，消除风险。

医疗卫生机构应当配合网信部门与公安机关开展医疗卫生机构数据安全事件核查调查。

第三十一条 地方各级卫生健康行政部门不履行本办法规定的数据安全和个人信息保护义务的，由其上级机关责令改正；对直接负责的主管人员和其他直接责任人员依法依纪给予处分。

第三十二条 医疗卫生机构违反《中华人民共和国基本医疗卫生与健康促进法》规定，因医疗信息安全制度、保障措施不健全，导致医疗信息泄露的，由县级以上人民政府卫生健康等主管部门责令改正，给予警告，并处以罚款；情节严重的，可以责令停止相应执业活动，对直接负责的主管人员和其他直接责任人员依法追究法律责任。

医疗卫生机构的相关人员泄露公民个人信息的，由县级以上人民政府卫生健康行政主管部门依照有关执业医师、护士管理、个人信息保护等法律、行政法规的规定予以行政处罚，属于政府举办的医疗卫生机构中的人员的，依法给予处分。

非法收集、使用、加工、传输公民个人健康信息，非法买卖、提

供或者公开公民个人健康信息等，构成违反治安管理行为的，依法给予治安管理处罚。

第三十三条 违反《中华人民共和国民法典》规定，泄露患者的隐私和个人信息，或者未经患者同意公开其病历资料的，应当承担侵权责任。

第三十四条 根据《中华人民共和国数据安全法》规定，各级卫生健康行政部门在履行医疗卫生机构数据安全监管职责中，发现数据处理活动存在较大安全风险的，可以按照规定的权限和程序对有关医疗卫生机构进行约谈，并要求医疗卫生机构采取措施进行整改，消除隐患。

医疗卫生机构违反《中华人民共和国数据安全法》，不履行规定的数据安全保护义务，或者向境外提供重要数据的，按照有关条款予以处理。

第三十五条 根据《中华人民共和国个人信息保护法》规定，各级卫生健康行政部门、网信部门和公安机关在履行职责中，发现医疗卫生机构存在较大风险或者发生个人信息安全事件的，可以按照规定的权限和程序对该医疗卫生机构的法定代表人或者主要负责人进行约谈，或者要求医疗卫生机构委托专业机构对其个人信息处理活动进行合规审计。医疗卫生机构应当按照要求采取措施，进行整改，消除隐患。卫生健康等履行个人信息保护职责的部

门在履行职责中，发现违反《中华人民共和国个人信息保护法》规定的，按照《中华人民共和国个人信息保护法》相关规定处理，发现违法处理个人信息涉嫌犯罪的，应当及时移送公安机关依法处理。

第三十六条 任何组织、个人有权对违法个人信息处理活动向卫生健康等履行个人信息保护职责的部门进行投诉、举报。收到投诉、举报的部门应当依法及时处理，并将处理结果告知投诉、举报人。卫生健康等履行个人信息保护职责的部门应当公布接受投诉、举报的联系方式。

第七章 附 则

第三十七条 开展涉及国家秘密、工作秘密的数据处理活动，适用《中华人民共和国保守国家秘密法》等法律、行政法规的规定。

第三十八条 医疗卫生机构可以根据本办法制定相应的实施细则。

第三十九条 本办法由国家卫生健康委负责解释。

第四十条 本办法自印发之日起施行。

国家卫生健康委办公厅　　2026年2月14日印发

校对：田东岳