国家健康医疗大数据标准、安全和服务管理办法

（试行）

**第一章 总则**

　　第一条 为加强健康医疗大数据服务管理，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，根据《中华人民共和国网络安全法》等法律法规和《国务院促进大数据发展行动纲要》《国务院办公厅关于促进和规范健康医疗大数据应用发展的指导意见》《国务院办公厅关于促进“互联网+医疗健康”发展的意见》等文件精神，就健康医疗大数据标准、安全和服务管理，制定本办法。

　　第二条 我国公民在中华人民共和国境内所产生的健康和医疗数据，国家在保障公民知情权、使用权和个人隐私的基础上，根据国家战略安全和人民群众生命安全需要，加以规范管理和开发利用。

　　第三条 坚持以人为本、创新驱动，规范有序、安全可控，开放融合、共建共享的原则，加强健康医疗大数据的标准管理、安全管理和服务管理，推动健康医疗大数据惠民应用，促进健康医疗大数据产业发展。

　　第四条 本办法所称健康医疗大数据，是指在人们疾病防治、健康管理等过程中产生的与健康医疗相关的数据。

　　第五条 本办法适用于县级以上卫生健康行政部门（含中医药主管部门，下同）、各级各类医疗卫生机构、相关单位及个人所涉及的健康医疗大数据的管理。

　　第六条 国家卫生健康委员会（含国家中医药管理局，下同）会同相关部门负责统筹规划、指导、评估、监督全国健康医疗大数据的标准管理、安全管理和服务管理工作。县级以上卫生健康行政部门会同相关部门负责本行政区域内健康医疗大数据管理工作，是本行政区域内健康医疗大数据安全和应用管理的监管单位。

　　各级各类医疗卫生机构和相关企事业单位是健康医疗大数据安全和应用管理的责任单位。

**第二章 标准管理**

　　第七条 健康医疗大数据标准管理工作遵循政策引领、强化监督、分类指导、分级管理的原则。

　　第八条 国家卫生健康委员会负责统筹规划、组织制定全国健康医疗大数据标准，监督指导评估标准的应用工作，在已有的基础性通用性大数据标准基础上组织制定健康医疗大数据标准体系规划，负责制定、组织实施年度健康医疗大数据标准工作计划。省级卫生健康行政部门（含省级中医药主管部门）负责监督指导评估本地区健康医疗大数据标准的应用工作，依据国家健康医疗大数据标准体系规划，结合本地实际，负责指导和监督健康医疗大数据标准体系在本省域内落地执行。

　　第九条 国家卫生健康委员会鼓励医疗卫生机构、科研教育单位、相关企业或行业协会、社会团体等参与健康医疗大数据标准制定工作。公民、法人或者其他组织可提出制修订健康医疗大数据标准的立项建议，并提交相应标准项目建议书。

　　第十条 国家卫生健康委员会负责统一组织实施，择优确定健康医疗大数据标准起草单位和负责人，提倡多方参与协作机制，由各相关单位组成协作组参与标准起草工作。

　　第十一条 健康医疗大数据标准起草、审查及发布的程序和要求，按照国家和行业有关规定执行。

　　第十二条 卫生健康行政部门应当对健康医疗大数据标准的实施加强引导和监督，充分发挥各级各类医疗卫生机构、相关企业等市场主体在标准应用实施中的积极性和主动性，建立激励和促进标准应用实施的长效管理机制。

　　第十三条 卫生健康行政部门应当建立相应的健康医疗大数据标准化产品生产和采购的激励约束机制，卫生健康行政部门要积极推进健康医疗大数据标准规范和测评工作，并将测评结果与医疗卫生机构评审评价挂钩。

　　第十四条 国家卫生健康委员会加强健康医疗大数据技术产品和服务模式的标准体系及制度建设，组织对健康医疗大数据标准应用效果评估工作，并根据评估情况，对相关标准进行组织修订或废止等。

　　第十五条 国家卫生健康委员会基于卫生标准管理平台，动态管理健康医疗大数据标准的开发与应用，对各级各类医疗卫生机构和企事业单位的标准应用情况进行动态监测。

**第三章 安全管理**

　　第十六条 健康医疗大数据安全管理是指在数据采集、存储、挖掘、应用、运营、传输等多个环节中的安全和管理，包括国家战略安全、群众生命安全、个人信息安全的权责管理工作。

　　第十七条 责任单位应当建立健全相关安全管理制度、操作规程和技术规范，落实“一把手”责任制，加强安全保障体系建设，强化统筹管理和协调监督，保障健康医疗大数据安全。

　　涉及国家秘密的健康医疗大数据的安全、管理和使用等，按照国家有关保密规定执行。责任单位应当建立健全涉及国家秘密的健康医疗大数据管理与使用制度，对制作、审核、登记、拷贝、传输、销毁等环节进行严格管理。

　　第十八条 责任单位应当采取数据分类、重要数据备份、加密认证等措施保障健康医疗大数据安全。责任单位应当建立可靠的数据容灾备份工作机制，定期进行备份和恢复检测，确保数据能够及时、完整、准确恢复，实现长期保存和历史数据的归档管理。

　　第十九条 责任单位应当按照国家网络安全等级保护制度要求，构建可信的网络安全环境，加强健康医疗大数据相关系统安全保障体系建设，提升关键信息基础设施和重要信息系统的安全防护能力，确保健康医疗大数据关键信息基础设施和核心系统安全可控。健康医疗大数据中心、相关信息系统等均应开展定级、备案、测评等工作。

　　第二十条 健康医疗大数据相关系统的产品和服务提供者应当遵守国家有关网络安全审查制度，不得中断或者变相中断合理的技术支持与服务，并应当为健康医疗大数据在不同系统间的交互、共享和运营提供安全与便利条件。

　　第二十一条 责任单位应当依法依规使用健康医疗大数据有关信息，提供安全的信息查询和复制渠道，确保公民隐私保护和数据安全。

　　第二十二条 责任单位应当按照《中华人民共和国网络安全法》的要求，严格规范不同等级用户的数据接入和使用权限，并确保数据在授权范围内使用。任何单位和个人不得擅自利用和发布未经授权或超出授权范围的健康医疗大数据，不得使用非法手段获取数据。

　　第二十三条 责任单位应当建立严格的电子实名认证和数据访问控制，规范数据接入、使用和销毁过程的痕迹管理，确保健康医疗大数据访问行为可管、可控及服务管理全程留痕，可查询、可追溯，对任何数据泄密泄露事故及风险可追溯到相关责任单位和责任人。

　　第二十四条 建立健全健康医疗大数据安全管理人才培养机制，确保相关从业人员具备健康医疗大数据安全管理所要求的知识和技能。

　　第二十五条 责任单位应当建立健康医疗大数据安全监测和预警系统，建立网络安全通报和应急处置联动机制，开展数据安全规范和技术规范的研究工作，不断丰富网络安全相关的标准规范体系，重点防范数据资源的集聚性风险和新技术应用的潜在性风险。发生网络安全重大事件，应当按照相关法律法规和有关要求进行报告并处置。

**第四章 服务管理**

　　第二十六条 国家卫生健康委员会负责制定健康医疗大数据应用领域相关规范、标准，建立健康医疗大数据应用诚信机制和退出机制，制定健康医疗大数据挖掘、应用的安全和管理规范。

　　第二十七条 责任单位实施健康医疗大数据管理和服务，应当按照法律法规和相关文件规定，遵循医学伦理原则，保护个人隐私。

　　第二十八条 责任单位应当根据本单位健康医疗大数据管理的需求，明确相应的管理部门和岗位，按照国家授权，实行“统一分级授权、分类应用管理、权责一致”的管理制度，并建设相应的健康医疗大数据信息系统作为技术和管理支撑。

　　第二十九条 责任单位采集健康医疗大数据，应当严格执行国家和行业相关标准和程序，符合业务应用技术标准和管理规范，做到标准统一、术语规范、内容准确，保证服务和管理对象在本单位信息系统中身份标识唯一、基本数据项一致，所采集的信息应当严格实行信息复核终审程序，做好数据质量管理。

　　第三十条 责任单位应当具备符合国家有关规定要求的数据存储、容灾备份和安全管理条件，加强对健康医疗大数据的存储管理。健康医疗大数据应当存储在境内安全可信的服务器上，因业务需要确需向境外提供的，应当按照相关法律法规及有关要求进行安全评估审核。

　　第三十一条 责任单位选择健康医疗大数据服务提供商时，应当确保其符合国家和行业规定及要求，具备履行相关法规制度、落实相关标准、确保数据安全的能力，建立数据安全管理、个人隐私保护、应急响应管理等方面管理制度。

　　第三十二条 责任单位委托有关机构存储、运营健康医疗大数据，委托单位与受托单位共同承担健康医疗大数据的管理和安全责任。受托单位应当严格按照相关法律法规和委托协议做好健康医疗大数据的存储、管理与运营工作。

　　第三十三条 责任单位应当结合服务和管理工作需要，及时更新、甄别、优化和维护健康医疗大数据，确保信息处于最新、连续、有效、优质和安全状态。

　　第三十四条 责任单位发生变更时，应当将所管理的健康医疗大数据完整、安全地移交给承接延续其职能的机构或本行政区域内的卫生健康行政部门，不得造成健康医疗大数据的损毁、丢失和泄露。

　　第三十五条 责任单位向社会公开健康医疗大数据时，应当遵循国家有关规定，不得泄露国家秘密、商业秘密和个人隐私，不得侵害国家利益、社会公共利益和公民、法人及其他组织的合法权益。

　　第三十六条 责任单位应当加强健康医疗大数据的使用和服务，创造条件规范使用健康医疗大数据，推动部分健康医疗大数据在线查询。

　　第三十七条 国家卫生健康委员会负责按照国家信息资源开放共享有关规定，建立健康医疗大数据开放共享的工作机制，加强健康医疗大数据的共享和交换，统筹建设健康医疗大数据上报系统平台、信息资源目录体系和共享交换体系。

**第五章 管理监督**

　　第三十八条 卫生健康行政部门应当加强监督管理，对本行政区域内各责任单位健康医疗大数据安全管理工作开展日常检查，指导监督本行政区域内各责任单位数据综合利用工作，提高数据服务质量和确保安全。各级各类医疗卫生机构应当接入相应区域全民健康信息平台，传输和备份医疗健康服务产生的数据，并向卫生健康行政部门开放监管端口。

　　第三十九条 卫生健康行政部门应当加强监测评估，定期开展健康医疗大数据平台和服务商的稳定和安全测评及健康医疗大数据应用的安全监测评估，建立网络安全防护、系统互联共享、公民隐私保护等软件评价和安全审查保密制度。

　　第四十条 卫生健康行政部门会同相关部门建立健康医疗大数据安全管理工作责任追究制度。对于违反本办法规定的单位和个人，由主管部门视情节轻重予以约谈、督导整改、诫勉、通报批评、处分或提出给予处分的建议；构成违法的，移送司法部门依法追究法律责任。

**第六章 附则**

　　第四十一条 本办法自印发之日起施行。