关于加强本市卫生健康数据安全与授权运营的工作指引（试行）

（拟互联网公开征求意见稿）

第一章 总　则

第一条 （目的和依据）为深入贯彻落实党中央、国务院以及市委市政府决策部署，统筹安全与发展，构建本市卫生健康数据全生命周期安全治理体系，安全有序推进卫生健康数据合规流通，加快本市数据要素市场培育，推动数字经济发展新格局，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》《中华人民共和国密码法》《中华人民共和国生物安全法》《网络数据安全管理条例》《上海市数据条例》《公共数据资源授权运营实施规范（试行）》《国家健康医疗大数据标准、安全和服务管理办法（试行）》《上海市公共数据资源授权运营管理办法（征求意见稿）》以及网络安全等级保护制度等相关法律法规和部门规章，结合本市卫生健康工作实际，制定本文件。

第二条 （适用范围）本市辖区范围内卫生健康行业单位、其他有关机构及人员开展的卫生健康数据处理活动及其监督管理适用本文件。

第三条 （有关定义）本文件下列用语的含义：

（一）本文件所称的数据为网络数据（简称“数据”）。

（二）卫生健康数据，是指在人们疾病防治、健康管理、医学教育、医学研究、医疗服务、医疗管理、行业管理等过

程中产生的与卫生健康相关的数据。

（三）卫生健康个人数据，是指在医疗活动中，依法收集或者产生的，载有可识别自然人个人信息的卫生健康数据，不包括匿名化处理后的数据。

（四）卫生健康公共数据，是指行业单位在依法履行公共管理职责或者提供公共服务过程中收集或者产生的卫生健康数据。

（五）数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开、删除等。

第四条 （工作原则）坚持以“网络安全为基础，数据安全为核心”“最小授权”为原则，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，兼顾数据安全与发展，深化数据全生命周期安全管理，强化风险识别、监测预警、应急处置等能力，落实安全保护措施。

第二章 职责分工与主体责任

第五条 （责任分工）数据安全与授权运营工作的主要责任分工:

（一）行业主管部门：市卫生健康委负责本市卫生健康行业数据安全和个人信息保护工作的统筹规划、指导监管工作，并对数据授权运营工作进行伦理与合规监管。

（二）办医主体：各区卫生健康委、上海申康医院发展中心、复旦大学、上海交通大学、同济大学、海军军医大学、上海中医药大学、健康医学院、相关国企等办医主体，负责所辖行业单位数据安全与个人信息保护的指导监督，并对相

关授权运营数据进行成本核算。

（三）行业单位：医疗机构、运营机构、开发主体等相关行业单位，负责数据授权运营流程相关环节的数据安全和质量管理，承担数据安全和个人信息保护的主体责任。在政府监管下，做好授权运营数据上链、备案、流通、利用等工作。

（四）市卫生健康数字智能创新实验室：由市卫生健康委与市数据局共同指导成立，是本市卫生健康数据授权运营工作的具体实施机构，负责本市卫生健康数据授权运营工作的伦理和技术审核工作，推动并完善本市卫生健康数据授权运营相关制度和能力建设。

（五）监管部门：网信、公安、数据等部门依照有关法律法规，在各自职责范围内履行数据监督管理相关职能。

第六条 （领导责任制）行业单位应严格落实网络安全责任制，建立数据安全工作机制，单位主要负责人是本单位数据安全和个人信息保护的第一责任人，分管数据安全和个人信息保护的负责人是直接责任人，要建立“主要负责人负总责，分管负责人牵头抓”的领导责任制，逐级明确职责，做到分工明确、责任到人。不得通过委托工作、外包等方式转移、转嫁主体责任。

第七条 （数据安全管理制度）行业单位应建立数据全生命周期安全管理制度，针对不同级别数据，制定数据收集、存储、使用、加工、传输、提供、公开、删除等环节的具体分级防护要求和操作规程。

第八条 （数据安全主体责任）行业单位要按照“谁主管谁负责、谁收集谁负责、谁持有谁负责、谁批准谁负责、谁使用谁负责”的原则，明确数据安全职能部门，建立分级分层的责任体系，明确各方责任。按要求构建覆盖数据全生命周期和应用场景的安全治理体系，强化数据安全防护措施，履行数据安全保护义务，开展日常安全运维、网络安全等级保护测评、网络数据安全风险评估、商用密码应用安全性评估和安全教育培训等，确保信息系统安全与业务连续性。

第三章 数据安全管理

第九条 （数据收集、存储和传输）行业单位应依据法律法规规定的方式和期限收集、存储数据。涉及重要数据的信息系统需落实第三级及以上网络安全等级保护和商用密码应用“三同步一评估”要求，强化数据安全保护的技术措施和监测措施，保障存储、传输通道安全，防止数据被窃取和篡改，确保数据的完整性、保密性、真实性和可用性。

第十条 （数据使用和加工）行业单位应按照卫生健康数据分类分级要求，开展数据备案登记管理，采取访问控制、数据防泄露、操作审计等管控措施，确保数据在使用和加工过程中的安全、合规和可控。使用加工公民个人信息和重要数据，还应建立权限管理、日志留存审计、实时监控、告警阻断、应急处置、数据溯源等相关技术和管理机制。

第十一条 （数据公开、提供和删除）卫生健康数据未经审查和批准，不得擅自公开。行业单位应按照有关规定安全有序提供数据，明确数据目的、范围、类别、条件、方式、

期限、程序等，提供的数据应限于实现数据接收方处理目的的最小范围。行业单位在提供数据前，应分析研判可能对国家安全、公共利益产生的影响，存在显著负面影响或风险的，不得对外提供。行业单位相关部门和从业人员未经单位许可，不得私自留存或对外提供数据。行业单位应当建立数据删除制度，自行或者委托具有资质的第三方机构进行操作，对删除活动进行记录和留存，重点关注数据残留风险，确保数据无法被还原。

第四章 个人信息保护

第十二条 （最小化原则）行业单位收集个人信息应限于实现业务处理目的的最小范围，不得过度收集个人信息。不得在法律、行政法规规定的范围外收集、存储可识别个人身份的人脸、指纹、虹膜等生物识别信息。

第十三条 （权益保护）行业单位未经个人或其监护人同意，不得公开其姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪轨迹等信息，法律法规规定的除外。

行业单位在处理卫生健康个人数据时，应当采取去标识化、匿名化等措施，确保在不借助其他数据和新兴技术的情况下无法识别特定自然人。

第十四条 （告知义务）行业单位处理卫生健康个人数据前，应真实、准确、完整地向个人或其监护人、授权代理人等告知其个人信息的处理目的、处理方式、处理的个人信息种类、保存期限，法律法规规定的除外。

第五章 数字智能管理

第十五条 （智能安全）行业单位在应用人工智能服务时，应当加强对训练数据和训练数据处理活动的安全管理，聚焦模型安全、产品安全、环境安全、结果安全等，定期开展安全审计和风险评估，采取有效措施防范和处置数据安全风险，提高应对新兴安全威胁能力，确保人工智能服务的合规性、安全性和可靠性。

第十六条 （语料通用安全）行业单位在开展医学人工智能应用时，聚焦临床医学、公共卫生、健康管理、中医药等场景，充分利用循证医学知识库、临床指南、电子病历、中医学典籍、饮片、药房等多元化语料资源，提高对通用有害内容、误导信息的识别能力，提升针对医学人工智能恶意使用卫生健康数据的甄别与防范能力，降低数据在应用中潜在风险。

第六章 数据授权运营

第十七条 （供数单位）行业单位是卫生健康数据授权运营工作的主要供数单位，需加强网络安全管理，防止数据被非法获取、出售或不当利用。按要求对授权运营数据进行单位内部审核并同意，完成单位内部数据归集与上链，保障供给数据质量，并向市卫生健康数字智能创新实验室进行登记备案、报送有资质的第三方机构出具的风险评估报告等。

第十八条 （用数单位）最终数据产品或服务的需求交付方是数据授权运营工作的主要用数单位，应具备数据实施安全保护能力并遵守相关法律法规，按需向市卫生健康数字

智能创新实验室提出用数需求，明确数据目的、方式、范围、类别、期限等要求。

第十九条 （运营机构）数据授权运营工作由市政府确定并授权的相关机构开展。在行业和数据主管部门的指导下，建设运营公共数据社会化开发利用平台及安全可信专区环境，依法依规在授权范围内开展业务。协助供数单位开展数据清洗、去标识化、匿名化等基础数据治理工作，并提供全过程上链技术支持和质量监控，履行数据安全主体责任，健全管理制度，加强内控管理，落实卫生健康数据分类分级保护制度要求，治理后的数据提供开发主体使用。

第二十条 （开发主体）主要为社会面的相关经营主体，对运营机构交付的基础公共数据产品和服务进行再开发，可融合多源数据，提升数据产品和服务价值，完成最终数据需求交付，繁荣数据产业发展生态。

第七章 风险监测和应急处置

第二十一条 （防范供应链风险）行业单位委托运营机构和开发主体处理数据活动的，应与被委托机构签订服务合同或其他有约束力的协议，明确数据处理活动中各方数据安全管理和个人信息保护等责任。持续核验被委托机构的数据安全防护能力和相关资质，监督被委托机构以约定内容开展数据处理活动，防范数据安全管理风险。未经行业单位同意，被委托机构不得委托他人开展卫生健康数据处理工作。

第二十二条 （风险监测）行业单位应对数据安全威胁进行监测，及时整改，消除隐患，防止数据篡改、破坏、泄

露、非法获取、非法利用等安全事件发生。

第二十三条 （应急响应与处置）行业单位应强化协调联动，建立数据安全事件应急响应机制，制定应急预案，每年至少开展一次演练，根据演练结果对应急预案进行评估和改进，提升处置风险隐患及安全事件的能力。

第二十四条 （事件报告）发生数据安全事件时，行业单位应立即启动应急预案，依规向行业主管部门报告，做好现场保护、留存相关记录，为监管部门依法维护国家安全和开展侦查调查等活动提供协助。

第二十五条 （加强组织保障）行业单位应高度重视数据安全管理和个人信息保护工作，加强统筹领导、部门协同，强化业务交流，深化人才培养，保障资金投入，建立考核评价制度。鼓励有条件的行业单位将考核评价与绩效挂钩。

第八章 监督管理

第二十六条 （监测预警）数据安全主管和监管部门应联防联控，建立数据安全和个人信息保护监测预警、风险信息共享机制，适时向行业单位发布风险提示。

第二十七条 （监督检查）数据安全主管和监管部门应定期对行业单位开展监督检查，聚焦数据全生命周期安全管理和个人信息保护，开展常态化安全检查，提升行业单位风险防范能力。

第九章 附　则

第二十八条 发生个人信息和数据泄露，或者出现重大网络与数据安全事件，或者违反、未能正确履行数据安全职

责的，或者未经本市卫生健康数据授权运营程序擅自将数据提供给市场主体的，按照相关法律法规，逐级倒查，追究其相应责任。

第二十九条 涉及国家秘密、生物安全、生命遗传、数据跨境、核心数据、突发重大公共卫生、特殊人群等特殊情形的，按照相关法律法规、部门规章执行。

第三十条 本工作指引自印发之日起实施，试用期2年。