深圳市卫生健康数据管理办法

（征求意见稿）

第一章 总 则

1. 【制定目的及依据】

为了规范卫生健康数据活动，保护隐私和个人信息，促进卫生健康数据有序流动和开发应用，根据《中华人民共和国网络安全法》《国家健康医疗大数据标准、安全和服务管理办法》《深圳经济特区健康条例》等有关规定，结合本市实际，制定本办法。

1. 【适用范围】

本市辖区范围内卫生健康行政部门、医疗卫生机构、医疗卫生行业组织及其工作人员开展的卫生健康数据活动及其监督管理适用本办法。

涉及国家秘密信息的数据活动，按照国家有关规定执行。

1. 【卫生健康数据的定义】

本办法所称卫生健康数据，是指在疾病防治、健康管理、医学相关研究等过程中产生的与卫生健康相关的数据，包括个人卫生健康数据与非个人卫生健康数据。

本办法所称数据处理，包括数据的收集、传输、存储、使用、加工、共享、开放等行为。数据活动是指为实现特定目的开展的一个或多个数据处理及与其相关的其他行为。

1. 【卫生健康行政部门职责】

市卫生健康行政部门负责全市卫生健康数据活动的管理工作，统筹规划、指导、评估、监督全市卫生健康数据活动，建立健全卫生健康数据治理体系、管理制度和标准规范，在职责范围内组织开展卫生健康数据活动，推动卫生健康数据开发应用。

各区卫生健康行政部门负责辖区内卫生健康数据活动的管理工作，在职责范围内组织开展卫生健康数据活动，推动卫生健康数据开发应用。

1. 【医疗卫生机构职责】

医疗卫生机构负责本机构卫生健康数据活动的管理，建立完善本机构卫生健康数据管理制度，依法开展卫生健康数据活动。

1. 【卫生健康数据活动原则】

卫生健康数据活动应当坚持统筹管理、统一标准、依法处理、安全可控、开放融合、创新驱动的原则，符合伦理原则和规范要求。

鼓励企业、科研机构、高等院校等参与卫生健康数据科学研究和开发应用。

第二章 数据活动的一般规定

1. 【卫生健康数据中心】

市卫生健康行政部门组织建设、运营、维护市卫生健康数据中心，统一、集约、安全、高效管理全市卫生健康数据资源，支持智慧健康建设、数字健康产业发展，并纳入城市大数据中心统一规划、统一管理。

市卫生健康数据中心由市卫生健康信息化平台、大数据创新支撑平台等组成，按照“一数一源”原则，收集、存储全市健康管理、预防保健、医疗服务、疾病控制、医学科研、医学教学、行业管理等卫生健康数据，分类形成卫生健康资源配置、居民电子健康档案、电子病历、疾病和健康危险因素监测等卫生健康相关主题数据库，配置大数据分析挖掘、大数据共享管控、人工智能算法建模等通用工具。

各区卫生健康行政部门可以建设区卫生健康信息化平台，支持和促进本辖区卫生健康数据开发应用。区卫生健康信息化平台应当与市卫生健康信息化平台对接。

1. 【数据资源目录及规范】

市卫生健康行政部门制定并公布全市卫生健康数据资源目录以及卫生健康数据标准、数据安全、数据处理等相关规范。

各区卫生健康行政部门、医疗卫生机构可以在全市卫生健康数据资源目录的基础上制定本辖区、本单位卫生健康数据资源目录，并于15日内向上一级卫生健康行政部门备案；数据资源目录变更的，应当重新备案。

1. 【数据活动的总要求】

市、区卫生健康行政部门、医疗卫生机构（以下统称责任单位）应当在数据资源目录范围内按照卫生健康数据相关规范开展数据活动，并符合合法、正当、必要、安全的要求。

涉及人类遗传资源的卫生健康数据活动，还应当符合人类遗传资源管理的有关规定。

1. 【责任单位要求】

责任单位应当明确本单位卫生健康数据管理的分管负责人和责任部门，并配备专兼职工作人员。

1. 【数据治理要求】

市卫生健康行政部门按照使用部门、服务对象、主题信息、应用场景及涉密、隐私等属性对卫生健康数据资源进行分级分类。

责任单位应当开展以卫生健康数据资源分级分类为基础的数据治理工作，按照分级授权、分类应用、权责一致的原则，对数据活动进行规范，夯实数据资源开发利用和共享开发基础。

涉及批量数据的复制、传输、开放、共享或者销毁等重大操作的，应当实施日志审计。

1. 【个人数据处理的总要求】

责任单位对全市卫生健康数据资源目录以外的个人卫生健康数据进行处理的，应当征得当事人或者其监护人明示同意，法律、法规另有规定的除外。

1. 【疫情相关个人信息】

为疫情防控收集的个人信息，不得用于其他用途。未经当事人或者其监护人授权同意，任何责任单位及其工作人员不得公开被收集者姓名、年龄、身份证号码、电话号码、家庭住址等个人信息，但因疫情防控工作需要，经过处理无法识别特定个人且不能复原的除外。

1. 【伦理审查】

责任单位开展涉及人的生命科学和生物医学研究的卫生健康数据活动，应当按照有关规定经伦理审查批准。

1. 【数据活动委托约定】

责任单位可以委托符合条件的单位开展卫生健康数据活动。

责任单位应当与被委托单位签订委托协议和保密协议，明确委托数据处理的具体行为、涉及的数据范围、委托期限、委托结束后的数据销毁、双方的权利义务、数据安全责任、违约责任等，还应当要求被委托单位不得将数据处理再次委托第三方，并对被委托单位开展的数据活动进行监督。

第三章 数据收集、传输和存储

1. 【数据收集范围】

责任单位应当在卫生健康数据资源目录范围内，按照卫生健康数据相关规范开展数据收集；因特殊业务或者紧急情况需要收集目录范围外卫生健康数据的，经向上一级卫生健康行政部门备案后，可以临时收集。

1. 【个人数据收集、留存原则】

责任单位不得违反法律法规和双方的约定收集个人卫生健康数据。

原则上，除满足自身安全防范需要外，责任单位不得留存可提取人脸识别信息的原始图像等数据。

1. 【数据收集要求】

责任单位收集卫生健康数据，应当根据健康管理、预防保健、临床诊疗、疾病控制、科学研究、质量控制、评审评价、监督管理等实际需要，明确数据收集的目的、范围、期限、处理规则、安全管理措施等。

责任单位应当真实、准确、及时、完整收集卫生健康数据，加强数据质量控制。

1. 【安全传输与存储】

责任单位应当对数据传输、存储采取下列安全防护措施：

1. 对涉及工作秘密、商业秘密、隐私和个人信息、知识产权以及其他敏感信息等数据采用国密算法进行加密；

（二）采用由密码技术支持的网络传输通道保护机制,保障通信网络数据传输的完整性、保密性,并具备应急恢复能力；

（三）数据存储在境内安全可信的服务器上，选取安全性能、防护级别与其安全等级相匹配的存储载体；

（四）建立可靠的数据容灾备份机制，保证数据的有效归档、恢复和使用；

（五）对身份鉴别、安全策略、异地备份、系统恢复等重要操作实行安全审计；

（六）法律法规和网络安全部门、卫生健康行政部门等规定的其他措施。

1. 【数据出境】

个人健康数据和重要的非个人健康数据，原则上不得出境。因业务需要确需向境外提供数据的，责任单位应当依照相关法律法规进行安全评估，并审批备案；涉及能够识别或者推断居民个人身份的隐私和个人信息的，应征得本人或其监护人的同意。

1. 【医疗卫生机构职责】

除紧急救治外，医疗卫生机构为居民提供基本医疗、基本公共卫生服务时，应当要求其出示有效身份证件。

医疗卫生机构应当按照全市统一规范记录并在本机构或政务云上存储为居民提供健康管理、预防保健、医疗服务、疾病控制等健康服务信息，并按照卫生健康行政部门制定的接口规范、数据标准和质量控制等要求，将数据录入或者上传至卫生健康信息化平台。使用电子病历系统的医疗卫生机构还应当将患者的电子病历数据上传至卫生健康信息化平台。

医疗卫生机构应当按照市卫生健康行政部门的要求，在本单位信息系统中为实名就医的居民建立身份标识唯一、基本数据项一致的电子健康档案，记录为其提供的健康服务信息，并按照身份对照标准纳入卫生健康信息化平台的居民电子健康档案进行联网管理。

1. 【非医疗卫生机构职责】

鼓励产生卫生健康数据的非医疗卫生机构将卫生健康数据传输至卫生健康信息化平台。

第四章 数据使用、加工

1. 【数据使用、加工的合规性审查】

责任单位应当制定本辖区、本单位数据使用、加工合规性审查制度，对数据的使用、加工进行规范管理。

责任单位及其工作人员应当在授权范围和目的内使用、加工数据，不得使用、加工未经授权的数据。

1. 【数据访问日志】

责任单位应当建立电子实名认证和数据访问控制制度，防止数据泄露或者被非法使用。数据的访问日志应当保存6个月以上，对医学文书、医学证明文件和归档病历、电子健康档案的数据访问日志应当保存3年以上。

1. 【电子病历和电子健康档案的调阅】

责任单位在开展预防保健、健康管理、临床诊疗等医疗卫生服务时，可以依法调阅居民电子健康档案。

医疗卫生机构开展医疗服务时，除以下情形，调阅电子病历需经居民本人或者其监护人授权同意，法律法规另有规定的从其规定。

（一）医护人员为患者提供临床诊疗服务的；

（二）健康管理责任医师为签约居民提供健康管理服务；

（三）医疗紧急救治或突发公共卫生事件中居民本人无法及时完成授权的情形；

（四）法律法规规定可以调阅、借阅病历的其它情形。

1. 【电子病历和健康档案调阅安全要求】

责任单位在调阅居民的电子病历或者电子健康档案时，不得进行拍照、录像、截屏、拷贝和本地保存等操作，不得用于卫生健康以外的目的。

1. 【数字证书】

签署数字证书的电子医学文书、医学证明文件和电子病历与纸质医学文书、医学证明文件和病历具有同等法律效力。

1. 【数据使用的对外解释】

按照“谁使用、谁解释”的原则，由数据使用单位负责卫生健康数据使用的对外解释。

1. 【数据加工原则】

责任单位应当根据卫生健康数据资源分级分类管理要求对数据采取适当脱密脱敏措施，在不影响数据使用、加工的前提下，涉及隐私和个人信息的数据，不得直接显示。

1. 【安全保障】

责任单位在委托、授权数据使用、加工时，应当对数据安全进行评估，并采取下列安全措施，保障数据安全：

（一）根据数据使用、加工的实际需要，制定并执行符合最小必要原则的数据提取方案；

（二）采取必要措施保障数据交接安全；

（三）清理、销毁提取过程所产生的中间数据；

（四）保留数据使用过程中的申请、审批和销毁记录；

（五）其他必要的安全措施。

第五章 数据共享

1. 【卫生健康公共数据共享】

责任单位应当为依法履行卫生健康行政管理、卫生监督、社会医疗保险管理、药品监督等公共管理职能以及提供医疗救治、健康管理、预防保健、疾病控制等公共服务的有关国家机关、事业单位、医疗卫生机构或者其他组织提供所需的卫生健康公共数据。

卫生健康公共数据是指，市、区卫生健康行政部门、医疗卫生机构和医疗卫生行业组织在依法履行公共管理职能或者提供公共服务过程中收集或者产生的，以一定形式记录、保存的各类卫生健康数据。

1. 【公共数据共享负面清单】

卫生健康公共数据以共享为原则，不共享为例外。市卫生健康行政部门制定卫生健康公共数据共享负面清单，并实行动态管理。下列数据应当纳入共享负面清单，法律法规另有规定的除外：

（一）涉及工作秘密、商业秘密的数据；

（二）共享后可能危害国家安全、公共安全、经济安全、社会稳定、公众健康或者社会公共利益的数据；

（三）法律法规规定的其他不予共享的数据。

卫生健康公共数据共享分为主动共享和依申请共享。

1. 【公共数据主动共享方式及范围】

市、区卫生健康行政部门应当通过市、区公共数据资源共享交换平台，主动共享卫生健康资源，包括基本医疗卫生服务目录、标准和收费价格，医疗卫生公共信用，医疗卫生相关证照等数据和其他依法应当主动共享的卫生健康公共数据。

原则上，医疗卫生机构不直接提供主动共享卫生健康公共数据。

1. 【公共数据共享申请对接和登记】

责任单位应当建立公共数据依申请共享对接机制，做好数据共享申请的登记。

1. 【依申请共享数据的流程】

公共数据共享申请由数据生成单位负责受理，经本单位数据管理责任部门会同业务部门审核同意后方可共享；经审核不同意共享的，应当向申请单位说明理由。

涉及多个数据生成单位的数据共享申请，由数据生成单位的共同上级卫生健康行政部门负责受理。

1. 【数据共享协议】

责任单位依申请提供共享数据时，应当与申请方签订数据共享协议，明确双方权利义务，坚持最小必要原则共享数据，并采取必要安全措施，以及定期对共享数据进行安全审计。

1. 【个人卫生健康数据共享备案】

责任单位根据数据共享协议共享500例以上涉及隐私或个人数据的，应当自共享之日起15日内报上一级卫生健康行政部门备案。

第六章 数据开放

1. 【卫生健康数据开放】

 卫生健康数据开放坚持公平有序、安全可控、分类管理的原则，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。。

卫生健康数据开放包括向个人开放和向社会开放。

1. 【向个人开放】

责任单位应当向成年居民、未成年居民的监护人开放电子健康档案和电子病历，提供在线查询、复制、更新、使用、授权等功能，并通过数据水印等技术保障数据防篡改、防泄露、可追溯。

1. 【向社会开放的数据分类】

 向社会开放的卫生健康数据分为无条件开放、有条件开放和不予开放三类。

无条件开放数据是指，按照深圳市政务公开相关规定应当公开且不涉及隐私和个人信息的卫生健康数据。

有条件开放数据是指，可以部分开放或者需要按照特定条件开放给自然人、法人或者非法人组织的数据。

不予开放数据是指，涉及工作秘密、商业秘密、能够识别或者推断居民个人身份的隐私和个人信息、法律法规规定不得开放的数据，以及开放后可能危及国家安全、公共安全、经济安全、社会稳定的数据。

1. 【开放数据获取途径】

市卫生健康行政部门应当通过市政府公共数据开放平台向社会开放卫生健康无条件开放数据。

市卫生健康行政部门依托卫生健康数据中心的大数据创新支撑平台开放卫生健康有条件开放数据，向有数据需求且具备相应数据处理能力的专业机构提供安全可靠的卫生健康数据开发利用环境，专业机构不得在该平台外处理数据。

原则上，区卫生健康行政部门和医疗卫生机构仅开放本辖区、本单位无条件开放数据。

1. 【开放数据的使用协议】

市卫生健康行政部门开放卫生健康有条件开放数据，应当与数据使用单位签订数据使用协议，并予以定向开放。协议应当明确数据的使用目的、性质、期限、范围、条件、数据产品、保密责任和安全措施等，且要求数据使用单位不得将获取的数据直接用于营利性活动。

1. 【禁止个人身份再识别处理】

禁止任何单位和个人以再识别或者推断居民个人身份为目的，对卫生健康开放数据进行数据处理。

第七章 安全和监管

1. 【安全责任】

责任单位应当严格落实网络安全主体责任，制定数据安全管理制度和数据安全应急预案，定期开展数据安全评测、风险评估和应急演练，保障卫生健康数据安全，履行个人信息保护职责。

1. 【相关信息系统网络安全等级保护】

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，加强卫生健康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。卫生健康大数据中心、卫生健康信息化平台、相关信息系统等均应开展网络安全定级、备案、测评等工作。

1. 【安全事件处理】

责任单位应当建立安全预警和信息报告制度，加强日常检查和监测预警，及时发现数据泄露等异常情况。

发生数据安全事件的，责任单位应当立即启动应急预案，采取补救措施，按照规定及时向数据主管部门和上一级卫生健康行政部门报告，并依法告知可能受到不利影响的单位或者个人。

1. 【监管职责】

市、区卫生健康行政部门应当加强对卫生健康数据活动的监督检查，对责任单位的数据报送情况、数据质量、数据应用等进行考核评估。

1. 【违法处罚】

责任单位及其工作人员违反本办法规定的，依照《中华人民共和国网络安全法》《深圳经济特区健康条例》等有关规定依法处理。

第八章 附 则

1. 【施行日期】

本办法自××××年×月×日起试行，有效期三年。