深圳市卫生健康数据管理办法

（再次征求意见稿）

第一章 总 则

第一条 为了规范卫生健康数据活动，保障数据安全，维护个人和组织的合法权益，促进卫生健康数据有序流动和开放共享，根据《中华人民共和国个人信息保护法》《中华人民共和国数据安全法》《深圳经济特区医疗条例》《深圳经济特区数据条例》等法律法规规定，结合本市卫生健康工作实际，制定本办法。

第二条 本市辖区范围内卫生健康行政部门、医疗卫生机构及其工作人员开展的卫生健康数据处理活动及其监督管理适用本办法。

涉及国家秘密的数据处理活动，按照国家有关规定执行。

第三条 本办法中下列用语的含义：

（一）卫生健康数据，是指在疾病防治、健康管理、医学教学和科研、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。

（二）卫生健康公共数据，是指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，以一定形式记录、保存的卫生健康数据。

（三）卫生健康个人数据，是指依法收集或者产生的，载有可识别特定自然人信息的卫生健康数据，不包括匿名化处理后的数据。

（四）卫生健康敏感个人数据，是指一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的卫生健康个人数据，以及不满十四周岁未成年人的卫生健康个人数据。

（五）数据处理，是指数据的收集、存储、使用、加工、传输、提供、公开、删除等行为。

第四条 市卫生健康行政部门依法负责全市卫生健康数据处理的管理工作，统筹规划、指导、评估、监督全市卫生健康数据处理活动，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处理活动，推动卫生健康数据开放共享。

区卫生健康行政部门依法负责辖区内卫生健康数据处理的管理工作，在职责范围内组织开展卫生健康数据处理活动，推动卫生健康数据开放共享。

第五条 医疗卫生机构依法负责本单位卫生健康数据处理的管理工作，建立完善本单位卫生健康数据管理制度，开展卫生健康数据处理活动。

第六条 本办法第四条、第五条规定的单位（以下统称责任单位）应当按照分类应用、分级授权、权责一致的原则对卫生健康数据处理活动进行规范管理，履行数据安全保护义务，不得损害国家利益、公共利益以及其他组织或者个人的合法权益，并符合合法、正当、必要、安全的要求。涉及生物安全的卫生健康数据处理活动，还应当符合生物安全管理的有关规定。

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 数据处理的一般规定

第七条 市卫生健康行政部门依托城市大数据中心组织建设、运营、维护深圳市卫生健康数据中心（以下简称市卫生健康数据中心）。市卫生健康数据中心按照“一数一源”原则，收集、存储全市卫生健康数据，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，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。

市、区卫生健康行政部门分别建设市、区卫生健康信息化平台，实现卫生健康数据互通共享，并将卫生健康数据汇聚至市卫生健康数据中心统一管理。

第八条 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，并配备专职或者兼职工作人员，建立健全本单位数据管理制度，组织开展数据安全和个人信息保护教育培训，落实数据安全保护责任。

第九条 市卫生健康行政部门制定并公布全市卫生健康公共数据资源目录以及卫生健康数据标准、安全和处理等相关规范，按照有关规定对卫生健康数据实行分类分级及安全管理，并将卫生健康公共数据资源纳入深圳市公共数据资源目录体系管理，规范卫生健康公共数据共享目录和开放目录。

第十条 卫生健康行政部门为履行法定职责处理卫生健康个人数据的，应当在处理前集中公告个人数据处理规则；个人数据处理规则未规定的，应当依法向个人告知。

医疗卫生机构处理卫生健康个人数据的，应当在处理前依法向个人进行告知，并取得个人或者其监护人的明确同意，涉及卫生健康个人敏感数据的，应当取得单独同意。法律、行政法规另有规定的除外。

第十一条 责任单位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和财产安全需要处理卫生健康个人数据的，应当按照最小必要原则，在法律法规规定的范围内进行数据处理，不得用于其他用途。

未经个人或者其监护人同意，责任单位及其工作人员不得公开其姓名、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、行踪信息等信息，因应对突发公共卫生事件需要且经匿名化处理的除外。

第十二条 责任单位进行卫生健康数据处理时，应当按照有关规定实施合规审计。开展涉及人的生命科学和生物医学研究的卫生健康数据处理活动，应当按照有关规定进行伦理审查。

第十三条 责任单位按规定委托相关单位开展卫生健康数据处理活动的，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目的、期限、处理方式、涉及的数据范围和种类、委托结束后的数据删除、数据安全保护措施和责任、违约责任等双方权利义务，并应当明确未经责任单位同意，被委托单位不得将数据处理转委托第三方处理。责任单位应当对被委托单位开展数据活动进行监督。

第三章 数据收集、传输和存储

第十四条 责任单位收集卫生健康数据时，应当根据工作需要，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、按时、完整收集卫生健康数据，加强数据质量控制。

第十五条 责任单位在收集、存储卫生健康个人数据时，应当依法告知当事人数据收集和存储的必要性、目的、范围、期限、处理规则以及对个人权益的影响，并按规定取得当事人同意，且不得违反法律法规规定和双方的约定。

责任单位不得在法律、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。

第十六条 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、知识产权和个人信息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、机密性，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、规章和网络安全部门、卫生健康行政部门等规定的其他措施。

第十七条 医疗卫生机构应当按照深圳市居民电子健康档案管理规范要求，在本机构信息系统中为实名就医的个人建立身份标识唯一、基本数据项一致的居民电子健康档案，记录为其提供的健康服务信息，并按照全市统一的接口规范、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，实现居民电子健康档案联网管理。

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实现联网管理。

第十八条 鼓励产生卫生健康数据的企事业单位、科研机构等其他单位将卫生健康数据按照规范传输至市卫生健康数据中心。

第四章 数据使用、加工和删除

第十九条 责任单位应当制定本辖区、本单位数据使用、加工的权限管理制度，责任单位工作人员应当在权限范围内使用、加工数据。

第二十条 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，对居民电子健康档案、医学证明文件、归档电子病历以及其他医学文书的数据访问日志应当保存3年以上。

第二十一条 医疗卫生机构为居民提供预防保健、健康管理、临床诊疗、互联网诊疗等医疗卫生服务时，经个人或者其监护人同意，可以依法查阅其居民电子健康档案。

符合下列情形之一的，医疗卫生机构可以依法查阅个人电子病历：

（一）个人或者其监护人单独同意；

（二）为居民提供医疗卫生服务时，查阅其在本机构以及属于同一法人单位的医疗机构的电子病历；

（三）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；

（四）法律、行政法规规定的其他情形。

第二十二条 医疗卫生机构基于个人同意查阅居民电子健康档案和个人电子病历的，应当由个人或其监护人在充分知情的前提下自愿、单独同意。个人或者其监护人可以选择下列同意方式：

（一）同意医疗卫生机构为个人提供本次卫生健康服务时查阅；

（二）同意医疗卫生机构为个人提供卫生健康服务时均可以查阅。

医疗卫生机构取得前款规定的个人同意的，个人或者其监护人有权撤回其同意，医疗卫生机构应当提供便捷的撤回同意的方式。个人撤回同意的，不影响撤回前基于个人同意已进行的个人信息处理活动的效力。

第二十三条 医疗卫生机构在查阅居民电子健康档案或者个人电子病历时，不得进行拍照、录像、截屏、复制和本地保存等操作，不得用于卫生健康以外的目的。法律、行政法规另有规定的除外。

第二十四条 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安全；

（三）及时清理、删除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、审批和删除记录；

（五）其他必要的安全措施。

第二十五条 对数据加工过程中临时保存的数据，以及保存或者使用期限届满后的数据，责任单位应当采用无法还原的方式及时进行删除，并验证数据删除操作的可信性，重点关注数据残留风险及数据备份风险。法律、法规另有规定的除外。

数据删除的审批流程、操作记录等资料应当存档保存。

第二十六条 按照“谁使用、谁负责、谁解释”的原则，由数据使用者负责卫生健康数据使用的对外解释。数据使用者应当收集数据使用过程中出现的问题，并积极与数据提供者协商处理。

第五章 数据共享和开放

第二十七条 责任单位应当建立卫生健康公共数据的共享对接机制，在卫生健康公共数据共享目录范围内，应有关国家机关、事业单位、医疗卫生单位等公共管理和服务机构的申请，依法共享卫生健康公共数据，并做好登记和管理。

第二十八条 责任单位应当要求卫生健康公共数据共享申请单位列明申请的数据字段，明确数据使用的依据、目的、范围、方式、期限等，并要求其按照规定加强共享数据使用管理，不得超出使用范围、期限或者用于其他目的。

责任单位依据规定的共享条件以及申请单位履行职责的需要进行审核，核定应用业务场景、用数单位、所需数据、共享模式、截止时间等等要素，按照最小授权原则，确保卫生健康公共数据按需、安全共享。

第二十九条 责任单位共享数据涉及卫生健康个人数据的，应当取得个人或者其监护人的单独同意，因履行法定职责或者法定义务所必需、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和财产安全所必需的除外。

第三十条 申请共享卫生健康公共数据涉及卫生健康个人数据的，责任单位应当要求申请单位提供以下资料：

（一）收集处理卫生健康个人数据的法律、法规、规章依据；

（二）提供明确的所需共享数据的人员名单；

（三）数据接收方的名称、联系方式、处理目的、处理方式和个人信息的种类；

（四）限于实现处理目的所必要的最小范围、采取对个人权益影响最小的方式等个人信息保护措施。

（五）申请单位经责任单位授权，取得的申请共享的个人数据所涉个人或其监护人作出的明确同意资料，但符合法律、行政法规规定不需要个人同意的除外。

申请单位无法明确共享数据人员名单的，责任单位可以提供卫生健康公共数据共享查询接口，并与申请单位协商确定涉及个人的范围和触发数据共享查询的条件。

第三十一条 责任单位应当在卫生健康个人数据共享前，向数据所涉及个人或者其监护人发送信息告知数据接收方的名称、联系方式、处理目的和处理方式和个人信息的种类。

第三十二条 国家机关、事业单位申请共享卫生健康公共数据的，由卫生健康行政部门通过城市大数据中心的公共数据共享平台，按照规定提供共享。

第三十三条 区卫生健康行政部门、市属医疗卫生单位申请共享卫生健康公共数据的，由市卫生健康行政部门通过市卫生健康信息化平台，按照规定提供共享。

区属医疗卫生单位申请共享卫生健康公共数据的，由区卫生健康行政部门通过区卫生健康信息化平台，按照规定提供共享。

第三十四条 责任单位应当规范数据共享管理，对不能通过公共数据共享平台或者卫生健康信息化平台共享卫生健康公共数据的，依法提供数据共享，并履行个人信息保护职责。

第三十五条 下列卫生健康公共数据不予共享：

（一）除法律、行政法规另有规定外，涉及工作秘密、商业秘密、知识产权的数据；

（二）除法律、行政法规另有规定外，共享后可能危害国家安全、公共安全、经济安全、社会稳定、公众健康或者公共利益的数据；

（三）法律、法规规定的其他不予共享的数据。

第三十六条 卫生健康行政部门通过公共数据共享平台无条件共享基本医疗卫生服务目录、收费价格、医疗卫生公共信用信息、医疗卫生相关证照和其他依法应当主动公开的卫生健康公共数据。

第三十七条 公安机关、司法、人力资源社会保障部门、医疗保障部门、保险等部门，因办理案件或者社会保险审核等需要，直接向数源责任单位提出卫生健康数据需求的，责任单位应当依法予以提供。

第三十八条 卫生健康公共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、公共利益和个人、组织的合法权益。

第三十九条 责任单位应当向成年居民本人、未成年人的监护人开放居民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，并通过电子签名、数字水印等技术保障数据防篡改、防泄露、可追溯。

第四十条 责任单位通过公共数据开放平台向社会提供可机器读取的卫生健康公共数据，按照向社会开放条件分为无条件开放、有条件开放和不予开放三类。

无条件开放的卫生健康公共数据，是指按照政府信息公开等相关规定应当无条件向自然人、法人和非法人组织开放的公共数据。

有条件开放的卫生健康公共数据，是指按照特定方式平等开放给自然人、法人和非法人组织的卫生健康公共数据。

不予开放的卫生健康公共数据，是指涉及国家安全、商业秘密和个人隐私，或者法律、法规等规定不得开放的公共数据。

第四十一条 责任单位公开、提供和开放卫生健康数据时，应当评估可能带来的安全风险，并采取必要的安全防控措施。

第四十二条 任何组织和个人不得以再识别或者推断个人身份为目的对共享和开放的卫生健康数据进行数据处理。

第六章 安全和监管

第四十三条 责任单位应当严格落实数据安全主体责任，制定数据安全管理制度和数据安全应急预案，定期开展数据安全测评、风险评估和应急演练，保障卫生健康数据安全。

第四十四条 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，加强卫生健康数据相关系统安全保障体系建设，开展网络安全定级、备案、测评等工作，提升关键信息基础设施和重要信息系统的安全防护能力。

第四十五条 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，并依法及时告知相关组织或者个人。

第四十六条 卫生健康行政部门应当加强对卫生健康数据处理活动的监督，对责任单位的数据报送情况、数据质量、数据应用等进行检查评估。

第四十七条 医疗卫生机构应结合工作实际，细化数据安全操作规程和技术规范，每年至少修订一次数据安全管理制度，与数据管理工作人员每年度签署保密协议。

第四十八条 责任单位及其工作人员违反本办法规定的，依据《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》《深圳经济特区数据条例》《深圳经济特区医疗条例》《深圳经济特区健康条例》等规定予以处理。

第七章 附 则

第四十九条 本办法自××××年×月×日起施行，有效期五年。