

# 上海市青浦区卫生健康委员会文件

青卫健信息〔2025〕2号

---

## 关于下发《青浦区卫生健康行业数据安全 管理实施细则（试行）》的通知

各医疗卫生机构：

为进一步规范本区卫生健康行业数据（以下简称“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《中华人民共和国数据安全法》《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》《上海市数据条例》《卫生健康数据分类分级要求》等法律法规和标准规范，参照青浦区数据局《上海市青浦区公共

数据安全管理办法（试行）》及上海市卫生健康委员会相关文件精神，结合本区卫生健康工作实际，制定了《青浦区卫生健康行业数据安全管理办法实施细则（试行）》，请各单位遵照执行。

附件：青浦区卫生健康行业数据安全管理办法实施细则（试行）

上海市青浦区卫生健康委员会

2025年5月23日

附件

# 青浦区卫生健康行业数据安全 管理实施细则（试行）

## 第一章 总则

### 第一条（目的依据）

为了规范本区卫生健康行业数据（以下简称“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《中华人民共和国数据安全法》《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》《上海市数据条例》《卫生健康数据分类分级要求》等法律法规和标准规范，参照青浦区数据局《上海市青浦区公共数据安全管理办法（试行）》及上海市卫生健康委员会相关文件精神，结合本区卫生健康工作实际，制定本实施细则。

### 第二条（适用范围）

本区卫生健康委员会（以下简称“区卫生健康委”）、医疗卫生机构及其工作人员开展的非涉密卫生健康数据处理活动及其监督管理适用本实施细则。

### 第三条（有关定义）

（一）卫生健康数据，是指在人们疾病防治、健康管理、医

学相关教学研究、医疗管理、监督执法等过程中产生的与卫生健康相关的数据。数据是指任何以电子或以其他方式对所处理信息的记录。

（二）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，载有可识别特定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。

（三）卫生健康公共数据，是指卫生健康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。

（四）数据处理者，是指开展数据处理活动的组织、个人。数据处理包括数据的收集、存储、使用、加工、传输、提供、共享、开放、流通、公开、删除等行为。

#### **第四条（工作原则）**

本区卫生健康数据安全工作坚持“网络安全为基础、数据安全为核心”原则，以“积极防御、综合防范”为要义，通过动态、多维度的防护体系应对复杂威胁，借助“原始数据不出域、数据可用不可见、数据可控可计量”等手段，严控数据安全风险。坚持安全与发展并重、管理与技术兼顾，实行统筹协调、分级管理、分工负责，与数字化项目同步规划、同步建设、同步运行、同步发展。

## 第二章 组织保障

### 第五条（领导小组）

（一）区卫生健康委成立区卫生健康数据安全工作领导小组，由委党政主要负责人任组长，是数据安全第一责任人；领导班子其他成员任副组长，其中分管数据安全的领导班子成员是直接责任人；各科室负责人为成员；信息化管理科为日常管理科室，具体负责本区卫生健康数据安全管理工作（详见附件）。

（二）本区医疗卫生机构应当成立本单位卫生健康数据安全管理工作领导小组，由单位党政主要负责人担任组长，指定分管领导和数据管理员，落实本单位数据安全管理工作。

## 第三章 职责分工

### 第六条（机构职责）

（一）区卫生健康委负责统筹规划、指导监管本区卫生健康数据安全管理和数据分类分级工作，审核汇总本区数据处理者梳理识别的数据情况。

（二）区卫生健康事业发展中心在职责范围内组织开展本区卫生健康数据处理活动，保障区域卫生信息共享交换平台数据安全，监督指导本区医疗卫生机构数据安全保障工作。

（三）本区医疗卫生机构负责本单位卫生健康数据处理和数据安全管理工作，建立健全本单位卫生健康数据安全管理制度

和工作规范，按“谁管业务，谁管数据，谁管数据安全”的原则开展卫生健康数据分类分级工作，对本单位卫生健康数据情况进行梳理和识别。

## **第四章 数据安全基本要素**

### **第七条（保护措施）**

本区医疗卫生机构应按照关键信息基础设施保护、网络安全等级保护等要求，对卫生健康数据实行分类分级管理，结合卫生健康数据全生命周期制定完善数据安全管控策略，通过管理和采取身份认证、授权访问、入侵防范、数据脱敏、数据加密、隐私计算、安全审计等各类技术手段，提高防病毒、防攻击、防篡改、防泄露、防窃取等防护能力。

### **第八条（风险监测）**

本区医疗卫生机构开展卫生健康数据处理活动时，应当加强数据安全风险监测，发现数据存在安全缺陷、安全漏洞等风险时，应当立即采取补救措施。

### **第九条（应急演练）**

本区医疗卫生机构应当建立卫生健康数据安全应急管理制度，制定应急处置预案，定期开展应急演练，并对演练情况进行评估，针对演练中发现的问题，修订完善应急预案。

### **第十条（应急处置）**

本区医疗卫生机构在发生卫生健康数据安全事件时，应当立即报告区卫生健康委，依照相关应急预案，采取应急处置措施，防止危害扩大，消除安全隐患，并及时公布与公众有关的警示信息。

### **第十一条（培训教育）**

本区医疗卫生机构应结合本单位实际，建立数据安全培训制度，定期组织开展具有针对性的卫生健康数据安全培训，不断提升本单位工作人员数据安全意识。

### **第十二条（风险评估）**

本区医疗卫生机构应对本单位实施的卫生健康数据处理活动每年定期开展风险评估，并向区卫生健康委报送风险评估报告。风险评估报告应当包括处理的重要数据的种类、数量，开展卫生健康数据处理活动的情况，面临的数据安全风险及其应对措施等。

### **第十三条（外包服务安全监管）**

本区医疗卫生机构通过服务外包形式开展数字化项目建设、运维或者开展卫生健康数据处理活动的，应与外包服务提供商签订数据安全保护和保密协议，双方共同承担数据安全责任，对外包服务提供商所有数据操作行为进行严格监管，并定期审计操作日志，对造成数据安全事故的依法追究 responsibility。

## 第五章 数据全生命周期安全管理

### 第十四条（数据采集安全）

（一）本区医疗卫生机构应当明确采集卫生健康数据的目的和用途，采集行为遵循目的正当、需求必要、方式合法、最小够用的原则，按照数据采集规范要求，依据法律法规规定的方式和期限在卫生健康数据资源目录范围内采集数据，不得过度采集。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。

（二）本区医疗卫生机构在数据采集过程中，应当对卫生健康数据采集的物理环境、技术工具等采取必要的安全管控措施，确保数据采集的准确性、完整性、可靠性和及时性，保证在采集过程中的数据不被泄露。在公共场所设置数据采集设施时，应当设置明显标识。

（三）本区医疗卫生机构在采集个人敏感信息时，应当获得被采集人的明示同意，提供有效的可替代选项和申诉机制，采取必要管理措施和技术手段保证被采集人能够终止采集行为，并删除已被采集信息，法律法规另有规定的除外。

### 第十五条（数据归集安全）

区卫生健康事业发展中心在数据归集的过程中，应当对数据归集的物理环境、技术工具等采取必要的安全管控措施，保护数

据在归集过程中不被泄露，确保数据归集的准确性、完整性、可靠性和及时性。

#### **第十六条（数据传输安全）**

本区医疗卫生机构应当制定并执行本单位卫生健康数据安全传输策略和规程，评估数据传输可能存在的安全风险，明确不同级别数据传输的安全要求，采取满足传输安全策略和数据安全等级的安全控制措施，确保数据传输的安全性和可靠性。

#### **第十七条（数据存储安全）**

本区医疗卫生机构应做好数据存储安全，明确数据备份和恢复操作规范。加强数据访问控制，根据用户需求和角色，设置不同的访问权限，制定包括身份标识、鉴别鉴权、认证授权、操作流程和终端设备的数据访问权限管理制度，明确不同身份权限可接触的数据类型、级别和量级，采用技术手段严格限制对个人敏感数据和重要数据的操作权限。

#### **第十八条（数据使用安全）**

本区医疗卫生机构涉及到个人敏感信息和重要数据使用时，应当采取单位内二次评估和授权，并做好数据脱敏与去标识化，对于敏感数据，在使用前进行脱敏处理，去除或替换关键信息。严格限制个人敏感信息和重要数据批量修改、复制、下载等重要操作权限，采用技术手段防止个人敏感信息和重要数据通过截屏、

复制等方式泄露。

### **第十九条（数据共享安全）**

区卫生健康事业发展中心应做好区域卫生信息共享交换平台数据共享工作，实现本区医疗卫生机构之间的数据交换，在数据共享过程中采用身份鉴别、访问控制等安全保障机制，确保获得授权的数据使用方访问共享数据。

### **第二十条（数据销毁安全）**

本区医疗卫生机构应落实安全可靠的数据销毁机制，确保以不可逆方式销毁敏感数据及其副本内容。在要求销毁或达到数据保存期限的情况下，应评估并审核数据销毁的业务必要性。进行销毁处理的同时应对数据销毁处理过程相关的操作进行记录，以满足安全审计的要求。

### **第二十一条（数据操作可溯）**

本区医疗卫生机构应在数据处理活动中记录并保存日志，确保所有数据操作行为可管可控，并保证审计日志的完整性和真实性。

## **第六章 数据分类分级**

### **第二十二条（数据分类规范）**

本区医疗卫生机构参照《WS/T 787-2021 国家卫生信息资源

分类与编码管理规范》，并在此基础上细化业务类别，制定本单位卫生健康数据分类表，将卫生健康数据分为基础资源类数据、业务资源类数据、主题资源类数据三大类。

### **第二十三条（数据分级规则）**

本区医疗卫生机构参照《DB31/T 1545-2025 卫生健康数据分类分级要求》制定本单位内部规则，将卫生健康数据分为核心数据、重要数据、一般数据三个级别。核心数据目录和重要数据目录按有关文件由国家主管部门确定，一般数据目录按上海市卫生健康委会、市中医药管理局、市疾控局等建议确定，一般数据目录建议与核心数据目录、重要数据目录存在冲突的，以国家主管部门发布的为准。

### **第二十四条（核心数据）**

核心数据是指对领域、群体、区域具有较高覆盖度或达到较高精度、较大规模、一定深度的重要数据，一旦被非法使用或共享，可能直接影响政治安全。卫生健康行业满足以下条件之一的重要数据，原则上应纳入核心数据的建议范围：

（一）1000 万人及以上个人信息或 100 万人及以上敏感个人信息；

（二）覆盖某一重要特定群体全部个体的数据，特定时期特定区域的群体数据；

(三) 涉及 1000 万人及以上，经过计算加工生成的，对数据描述对象有较深刻画程度，且影响国家安全的衍生数据；

(四) 其他经主管部门评估的核心数据。

## **第二十五条（重要数据）**

重要数据是指特定领域、特定群体、特定区域或达到一定精度和规模的数据，一旦被泄露或篡改、损毁，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全。仅影响组织自身或公民个体的数据，一般不作为重要数据。卫生健康行业满足下列条件之一，原则上应纳入重要数据的建议范围：

(一) 涉及 100 万人及以上个人信息或 10 万人及以上敏感个人信息；

(二) 全域性的业务数据，如涉及 10 万人的群体健康生理状况数据；涉及 1 万人的族群生物特征数据、医疗资源数据；涉及 10 万人的诊疗数据、医疗救援保障数据、特定药品实验数据等；

(三) 其他经主管部门评估的重要数据。

## **第二十六条（一般数据）**

一般数据是指核心数据、重要数据之外的其他数据。

## **第二十七条（数据级别更新）**

数据级别确定后，出现下列情形之一的，应对数据级别及时

更新：

（一）数据内容发生较大变化；

（二）数据内容未发生变化，但数据规模、数据时效性、数据应用场景、数据加工处理方式等发生较大变化；

（三）因国家有关要求，导致原定的数据级别不再适用；

（四）需要对数据级别进行变更的其他情形。

## **第二十八条（衍生数据分级）**

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，综合考虑数据加工处理后对数据规模、精度、深度的影响，重新评估确定数据级别。

## **第二十九条（数据分类分级方法）**

在数据分类的基础上，根据卫生健康数据的重要程度以及泄露后对不同对象造成的影响和危害程度，对卫生健康数据资源进行分级，数据分级参照以下步骤进行。

（一）确定影响对象：根据卫生健康数据遭受破坏后的影响对象来确定，包括国家安全、经济运行、社会秩序、公共利益、组织权益、个人权益。

（二）确定影响程度：根据卫生健康数据遭受破坏后所造成的影响程度来确定，包括特别严重危害、严重危害和一般危害。

（三）识别数据分级因素：数据分级过程中，应做好数据分

级因素的识别工作，包括领域、群体、区域、精度、规模、深度、覆盖度、安全风险等。

（四）确定数据级别：根据卫生健康数据遭受破坏后的影响对象和所造成的影响程度，对数据分级因素进行识别，依据就高从严原则确定数据级别。

### **第三十条（数据分类分级工作流程）**

（一）本区医疗卫生机构应对所掌握的数据进行全面梳理。涉及网络运行的，还应梳理网络安全等级保护和关键信息基础设施安全保护情况。

（二）本区医疗卫生机构对数据资源进行梳理（含数据基本情况、责任主体情况、数据处理情况和数据安全情况等），确定数据类别，识别数据级别，完成数据分类分级工作后，将数据资源清单上报区卫生健康委。

（三）本区医疗卫生机构的一般数据目录实施动态更新机制。需变更一般数据基本情况的，应在发生变化后的 30 日内重新实施分类分级流程。需变更一般数据基本情况之外信息的，应在发生变化后的 60 日内上报区卫生健康委。

## **第七章 数据开放管理**

### **第三十一条（数据公开）**

本区医疗卫生机构在履行职责中获悉的卫生健康和个人信

息等数据，应当依法予以保护，不得泄露或非法向他人提供。

### **第三十二条（数据提供）**

本区医疗卫生机构应按照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。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。本区医疗卫生机构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。

### **第三十三条（个人信息权益保护）**

本区医疗卫生机构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、行踪轨迹等卫生健康个人数据，法律法规规定的除外。

### **第三十四条（数据共享开放）**

数据使用方申请本区医疗卫生机构采集的卫生健康数据时，须明确数据使用目的、方式、范围、类别、期限等需求，经数据提供单位内部审核后共享开放，并向区卫生健康委登记备案。

数据使用方申请区卫生健康事业发展中心归集的卫生健康数据时，须明确数据使用目的、方式、范围、类别、期限等需求，经区卫生健康委审核后，通过区大数据资源平台或区卫生信息共

享交换平台获取数据。

本区医疗卫生机构对数据开放项目应进行伦理与技术双审核，确保数据开放安全、有序、合规。

## **第八章 数字智能管理**

### **第三十五条（智能安全）**

本区医疗卫生机构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，采取有效措施防范和处置数据安全风险。

### **第三十六条（语料通用安全）**

本区医疗卫生机构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、中医中药等场景，充分利用循证医学知识库、临床指南、电子病历、中医学典籍、药材药房等多种语料资源，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。

## **第九章 监督管理与责任追究**

### **第三十七条（监督检查）**

区卫生健康委组织开展本区医疗卫生机构常态化数据安全检查，对落实卫生健康数据分类分级保护等情况进行监督，发现存在较大安全风险的，按照规定权限和程序进行约谈、通报，并

要求其采取措施限期整改，消除隐患。

### **第三十八条（责任追究）**

对于本区医疗卫生机构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、未能履行数据安全职责的，按照相关法律法规，逐级倒查，依法追究其相应责任。

## **第十章 附则**

### **第三十九条（涉密规定）**

涉及数据跨境流动、国家秘密信息或者卫生健康数据汇聚关联后属于国家秘密事项的数据处理活动，应当符合国家相关保密规定。

### **第四十条（条款解释）**

本细则由区卫生健康委信息化管理科负责解释。

### **第四十一条（实施时间）**

本细则自发布之日起实施。

附件：青浦区卫生健康委数据安全工作领导小组名单

附件

## 青浦区卫生健康数据安全工作领导小组名单

组 长：	俞藕英	区卫生健康工作党委书记（第一责任人）
	胡 炯	区卫生健康委副主任（第一责任人）
副组长：	张 备	区卫生健康工作党委副书记
	吴金英	区卫生健康委副主任
	汪 畅	区卫生健康委副主任（直接责任人）
	费凤英	区卫生健康委副主任
	沈利群	区卫生健康委副主任
成 员：	张伟锋	区卫生健康委办公室主任
	高雅蓉	区卫生健康委组织人事科科长
	杨丽艳	区卫生健康委计划财务科科长
	杜懿杰	区卫生健康委医政管理科负责人
	张轶西	区卫生健康委中医科教科科长
	叶开友	区卫生健康委疾病预防科负责人
	黄 方	区卫生健康委综合监督科科长
	徐 喆	区卫生健康委基层卫生科科长
	沈佳颖	区卫生健康委家庭发展科科长
	程 东	区卫生健康委信息化管理科科长
	张 薇	区卫生健康委健康促进科科长
	周维娟	区卫生健康委审批办负责人

日常管理科室：信息化管理科

今后，青浦区卫生健康委数据安全工作领导小组成员如有变动，由接任者自然替换。