ICS 35.020
CCS 点击此处添加 CCS 号

T/YNCF

团　　体　　标　　准

T/YNCF XXX—XXXX

医院健康数据分类分级指南

点击此处添加标准名称的英文译名

（征求意见稿）

（本草案完成时间：2023 年 12 月 1 日）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

2023－XX－XX 发布　　2023－XX－XX 实施

云南省计算机学会　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文是云南省计算机学会数字医疗专业委员会提出的医院健康数据分类分级原则与方法，包括：数据分类分级基本原则、数据分类与分级框架等。适用于医疗机构开展健康数据安全分类分级工作，为数据安全管理和数据安全风险评估工作提供参考。数据分为核心数据、重要数据和一般数据三个级别，其中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，一旦泄露可能危害国家安全、经济运行、社会稳定和公共健康安全。核心数据是对领域、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。衍生数据包括去标识化和匿名化的脱敏数据、标签数据、统计数据和融合数据，其级别根据数据加工程度可进行升级或降级调整。数据分类分级实施流程包括数据资产梳理、数据分类、数据分级、审核发布、目录上报、动态更新管理。

本文件由云南省计算机学会提出。

本文件由云南省计算机学会归口。

本文件起草单位：

本文件主要起草人：

本文件首次提出。

引　言

医院健康数据是医疗信息的载体，它既有结构化信息，也有非结构化的自由文本和图形图像信息。国内公立二级及以上医院都具备一定的患者数据的采集与存储能力。医院健康数据，涉及个人身份信息、诊断数据、生命体征数据、治疗记录、用药记录等，既医疗机构的工作记录数据，也是个人隐私数据。这些数据全部或部份非授权使用可能导致对个人利益、机构利益、社会利益甚至国家安全的损害。对医院健康数据进行分级管理，有利于医疗机构科学、有序地界定数据的使用范围和应用权限划分。在大数据、物联网、AR等新技术的推动下，医院信息化建设飞速发展，智慧医疗进程加速，数据安全保障是核心支撑。

为贯彻落实《中华人民共和国数据安全法》，以及国家卫生健康委、国家中医药局、国家疾控局联合下发的《关于印发卫生健康行业数据分类分级指南（试行）的通知》的相关要求，对医院业务开展过程中的健康数据实施分类分级管理，进一步明确数据保护对象，助力医疗机构建立完善的健康数据生命周期保护框架，促进健康数据在医院内部、机构间、行业间的安全共享，特编制本指南。

医院健康数据分类分级指南

1 范围

本文件给出了医院健康数据分类分级的原则和方法，包括数据分类分级基本原则、数据分类框架和方法、 数据分级框架和方法等。

本文件适用于医疗业机构开展健康数据安全分类分级工作，并为医疗从业机构、第三方评估机构等单位开展数据安全管理和数据安全风险评估工作提供参考。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069-2022 信息安全技术 术语

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 39725-2020 信息安全技术 健康医疗数据安全指南

GB/T 41479-2022 信息安全技术 网络数据处理安全要求

TC260-PG-20212A 网络安全标准实践指南——网络数据分类分级指引

国卫办规划函 〖2023〗233号《卫生健康行业数据分类分级指南》（试行）

T/ISEAA 002-2021 信息安全技术 网络安全等级保护大数据基本要求

WS/T 787-2021 国家卫生信息资源分类与编码管理规范

3 术语和定义

下列术语和定义适用于本文件。

3.1 数据 Data

是指任何以电子或者其他方式对信息的记录。[来源：中华人民共和国数据安全法，第三条]。

3.2 医院健康数据 Hospital Health Data

指在疾病防治、健康管理、医学相关教学研究、医疗管理等过程中产生的数据。

[来源：卫生健康行业数据分类分级指南 第二条]。

3.3 衍生数据 Derived Data

经过统计、关联、挖掘、聚合、去标识化等加工活动而产生的数据。

注：根据数据的加工程度，可将衍生数据分为脱敏数据、标签数据、统计数据、关联数据等。

[来源： 信息安全技术 网络数据分类分级要求，3.8]

3.4 核心数据 Core Data

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。

[来源：卫生健康行业数据分类分级指南 第十三条]。

3.5 重要数据 Important Data

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。

[来源： 卫生健康行业数据分类分级指南 第十二条]

3.6 一般数据 General Data

是指核心数据、重要数据之外的其他数据。

[来源： 卫生健康行业数据分类分级指南 第十二条]

3.7 数据处理 Data process

数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等。

[来源：中华人民共和国数据安全法第三条] data process

3.8 数据分类 Data Classification

根据数据的属性或特征，将其按照一定的原则和方法进行区分和归类，并建立起一定的分类体系和排列顺序，以便更好地管理和使用数据的过程。

3.9 数据分级 Data Grading

按照数据遭到破坏后对国家安全、社会秩序、公共利益以及个人、法人和其他组织的合法权益（受侵害客体）的危害程度对数据进行定级，为数据全生命周期管理的安全策略制定提供支撑。

3.10 个人信息 Personal Information

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

注：个人信息包括但不限于自然人的姓名、出生日期、身份证件号码、住址、电话号码等。

3.11 个人敏感信息 Personal Sensitive Information

一旦泄漏、非法提供或滥用就有可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等个人信息。

3.12 公开披露 Public Disclosure

向社会或非特定人群发布信息的行为。

3.13 共享 Sharing

信息控制者向其他控制者提供信息，且双方分别对信息拥有独立控制权的行为。

4 数据分类分级原则

在遵循国家和医疗行业数据分类分级保护要求的基础上，依据以下原则进行分类和分级：

a) 合法合规原则：满足国家相关法律法规、技术标准及医疗行业主管监管部门有关规定要求，优先识别法律法规和医疗行业规定的数据类别；

b) 可执行性原则：数据分类分级规则要有利于数据管理和使用，避免过于复杂，以确保数据分类分级工作的可行性。

c) 关联性原则：数据分类是数据分级的基础，数据分类与分级密不可分。

d) 自主性原则：结合医疗业机构自身数据管理需要（如战略需要、业务需要、风险接受程度等），在本标准的框架下自主确定数据安全级别。

e) 分级明确原则：数据分级的目的是保护数据安全，数据分级的级别应界限明确，为不同级别的数据采取不同的保护措施提供依据。

f) 权限管理原则：体现权限授权的要素，反映内部控制的基本原则，对所属部门在生产经营活动中（包括内部和外部）发生的数据生产、访问与提取进行界定和管理。

g) 动态调整原则：数据的类别级别可能因时间变化、政策变化、安全事件发生、不同应用场景的敏感性变化或相关行业规则不同而发生改变，因此需要对数据分类分级进行定期审核并及时调整。

5 数据分类分级框架

5.1 分类分级范围

本指南仅适用于医院在健康数据处理活动中，对非涉密数据开展的分类分级工作。涉及国家秘密的数据按照国家有关规定执行。

5.2 数据分类

根据医疗行业数据特点，参考 WS/T 787-2021《 国家卫生信息资源分类与编码管理规范》，医院健康数据分类参考如下表，在实际数据分类过程中，各医院可根据实际情况做出相应调整。

医院健康数据分类表

数据一级类别	数据二级类别	数据三级类别
1 基础资源类	1.1 服务范围与对象	1.1.1 患者
		1.1.2 健康人
		1.1.3 医务人员

		1.1.4 管理者
	1.2 卫生健康信息化	1.2.1 全民健康信息平台
		1.2.2 医院信息平台
		1.2.3 应用系统
		1.2.4 数据接口
2 业务资源类	2.1 公共卫生	2.1.1 疾病控制
		2.1.2 卫生监督执法
		2.1.3 妇幼保健
		2.1.4 爱国卫生与健康促进
		2.1.5 医疗急救
		2.1.6 血液管理
		2.1.7 职业健康
	2.2 医疗服务（医院）	2.2.1 临床服务
		2.2.2 医疗管理
		2.2.3 运营管理
	2.3 医疗服务（基层）	2.3.1 基本医疗服务
		2.3.2 运营管理
		2.3.3 监管接口
	2.4 医疗保障	2.4.1 城镇居民基本医疗保险
		2.4.2 城镇职工基本医疗保险
		2.4.3 商业医疗保险
	2.5 药品供应	2.5.1 基础数据库管理
		2.5.2 采购项目管理
		2.5.3 采购目录管理
		2.5.4 采购计划管理
		2.5.5 分类采购
		2.5.6 合同管理
		2.5.7 供应管理
		2.5.8 结算支付
		2.5.9 价格管理
		2.5.10 公示公告
		2.5.11 统计查询
		2.5.12 综合监管
		2.5.13 信息交换共享
		2.5.14 高值医用耗材采购
	2.6 计划生育	2.6.1 全员人口
		2.6.2 流动人口
		2.6.3 精准扶助
		2.6.4 计生证件

3 主题类资源	3.1 全员人口数据库	3.1.1 全员人口信息
	3.2 电子病历数据库	3.2.1 业务运营
		3.2.2 临床诊疗
		3.2.3 电子病历
		3.2.4 基础字典
	3.3 电子健康档案数据保护	3.3.1 健康档案基本数据集
		3.3.2 疾病管理
		3.3.3 疾病控制
		3.3.4 儿童保健
		3.3.5 妇女保健
	3.4 医学研究数据库	3.4.1 医学研究基础信息
		3.4.2 医学研究科学数据
		3.4.3 医学研究成果数据
		3.4.4 其他医学研究数据
	3.5 其他数据库	3.5.1 电子病历摘要
		3.5.2 电子健康档案摘要
		3.5.3 人口基础信息共享
		3.5.4 远程医疗
		3.5.5 互联网+医疗健康
		3.5.6 家庭医生签约服务
		3.5.7 卫生健康综合管理
		3.5.8 医疗卫生监督
		3.5.9 公共卫生监督
		3.5.10 个人电子疾病档案
		3.5.11 健康危害因素
		3.5.12 疾控综合管理与爱国卫生资源管理服务
		3.5.13 疫苗和冷链管理
		3.5.14 医疗服务质量与绩效评价
		3.5.15 托育机构备案信息
		3.5.16 职业健康管理
4 衍生数据	4.1 衍生数据	4.1.1 个人信息衍生数据
		4.1.2 健康信息衍生数据
		4.1.3 疾控信息衍生数据

5.3 数据分级

医院健康数据分为核心数据、重要数据、一般数据三个级别，本指南主要用于识别认定重要数据和核心数据。

5.3.1 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。医院健康数据满足下列条件之一，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）全国性的业务数据，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）经评估的其他数据。

5.3.2 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。医院健康数据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）经评估的其他数据。

5.3.3 衍生数据

衍生数据分级，对照原始数据集开展，遵循就高从严原则，同时按照数据加工程度也可进行升级或降级调整。

--去标识化和匿名化的脱敏数据，级别可比原始数据集级别低。

--标签数据，级别可比原始数据集级别低。

--统计数据，如果结果数据涉及大规模群体特征或者宏观业务特征，可设置比原始数据集级别高。

--融合数据，若结果数据汇聚了更多的原始数据或挖掘出更敏感的数据，级别需要升高，如果结果数据降低了标识化程度等，级别可以降低。

6 数据分类分级实施流程

数据分类分级实施的主要步骤包括：

a）数据资产梳理：对数据资产进行全面梳理，包括以物理或电子形式记录的数据库表、数据项、数据文件等结构化和非结构化数据资产，明确数据资产基本信息和相关方，形成数据资产清单。

b）数据分类：按照数据分类分级有关要求，根据5.2 数据分类的规则，对数据进行分类，同时对个人信息、敏感个人信息进行识别和分类。

c）数据分级：按照数据分类分级有关要求，5.3数据分级规则，对数据进行分级。

d）审核发布：对数据分类分级结果进行审核和完善，最后批准发布执行。

e）目录上报：形成数据分类分级清单和重要数据、核心数据目录，按有关程序报送重要数据和核心数据目录等。

f）动态更新管理：根据数据重要程度和可能造成的危害程度变化，对数据分类分级规则、重要数据和核心数据目录、数据分类分级清单和标识等进行动态更新管理。需变更重要数据和核心数据基本情况的，应在发生变化后的 30日内重新实施分类分级流程。需变更重要数据和核心数据基本情况之外信息的，应在发生变化后的 60日内逐级上报至国家卫生健康委、国家中医药局、国家疾控局信息化主管司局备案。

实施流程图如下图 1 所示：

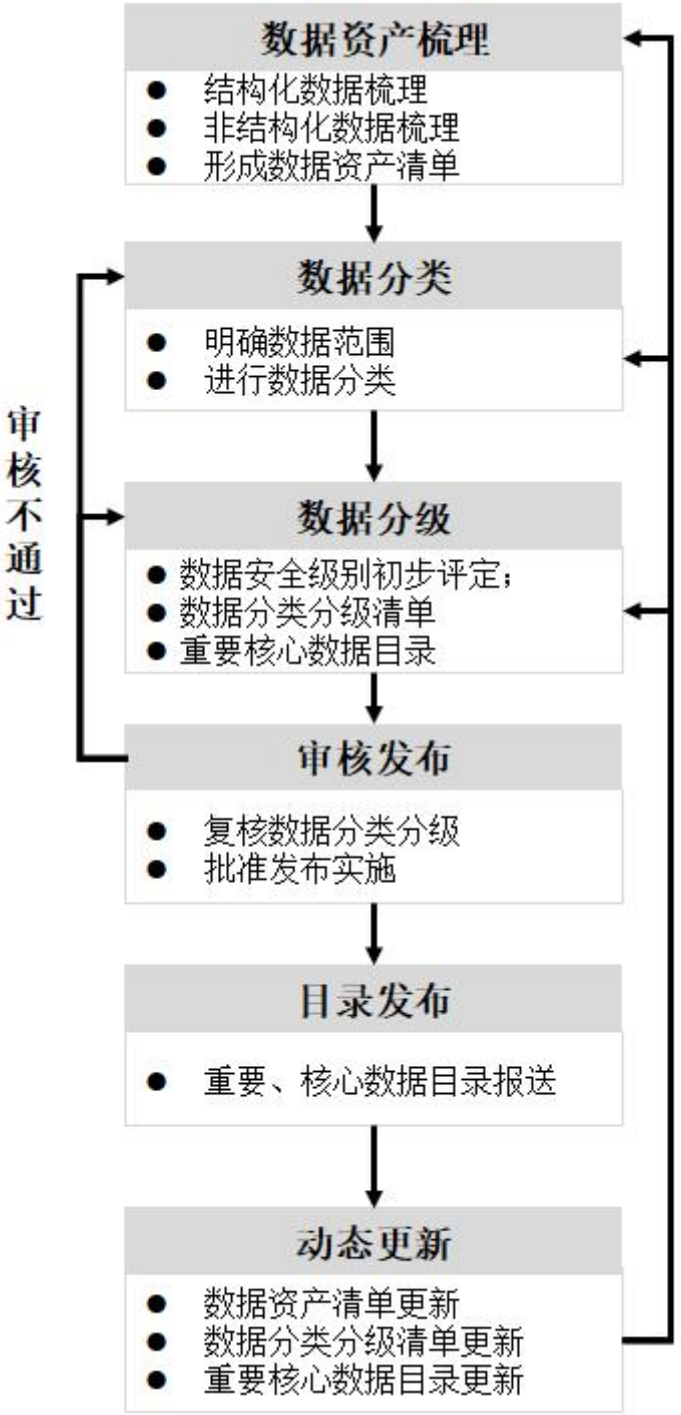

图1 数据分类分级实施流程

参 考 文 献

[1] GB / T 39725-2020 信息安全技术 健康医疗数据安全指南
[2] WS 445-2014 电子病历基本数据集标准
[3] DB31DSJZ005-2020 公共数据安全分级指南
[4] DB33/T 2351—2021 数字化改革 公共数据分类分级指南
[5] DB52/T1123-2021 政府数据 数据分类分级指南
[6] DB3301/T 0322.3—2020 数据资源管理 第3部分：政务数据分类分级
[7] JR/T 0197-2020金融数据安全 数据安全分级指南
[8] TC260-PG-20212A 网络安全标准实践指南——网络数据分类分级指引
[9] 健康医疗大数据安全管控分类分级实施指南
[10] 卫生健康行业数据分类分级指南（试行）