ICS 35.030
CCS L 80

团 体 标 准

T/GDWJ 024—2024

健康医疗信息 重要数据识别和管理指南

Health medical information-guideline for identification and management of key data

2024－05-09 发布 2024－05－09 实施

广东省卫生经济学会 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。

请注意本文体的某些内容可能涉及专利，本文件的发布机构不承担识别专利的责任。

本文件由广东省卫生经济学会提出并归口。

本文件起草单位：东莞市第六人民医院、东莞市卫生统计信息中心、广东网安科技有限公司、中山大学附属口腔医院、郑州立雪智能科技研究院、东莞市滨海湾中心医院、江门市中心医院、东莞市第八人民医院、清远市人民医院、连州市人民医院、中山大学附属第一医院、广东省妇幼保健院、广州医科大学附属第二医院、深圳市大数据研究院、广州医科大学附属口腔医院、广东省卫生经济学会、广州医科大学附属脑科医院、汕头市中心医院、佛山市第一人民医院、连州市医疗总院、暨南大学附属顺德医院、东莞市凤岗医院、广州市民政局精神病院、北京中安星云软件技术有限公司、深信服科技股份有限公司、福建中信网安科技有限公司、深圳君同云科技有限公司、杭州数圭通科技有限公司、杭州美创科技股份有限公司、深圳昂楷科技有限公司。

本文件主要起草人：熊劲光、郑金、陈惠城、魏书山、黄春柳、高峰、王映辉、涂华、温明峰、黄新萍、张敦明、冯海燕、陆慧菁、肖庆颖、张亮鸣、李永强、邓联丙、潘遂壮、邱扬、林晓怡、邓意恒、吴庆斌、冯成志、郑彤涛、董鹏翔、刘杰、袁征、阳磊、文琼、胡雪儿、黄帮钦、周卫华、刘永波、蔡明辉等。

引　言

2021年9月1日,《中华人民共和国数据安全法》正式施行,明确提出“各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的数据进行重点保护”；国家卫生健康委员会等部门2022年制定印发的《医疗卫生机构网络安全管理办法》也明确了“坚持分等级保护、突出重点。重点保障关键信息基础设施、网络安全等级保护第三级（以下简称第三级）及以上网络以及重要数据和个人信息安全”。

开展数据分类分级保护工作,需要在对数据进行分类分级的基础上重点识别涉及的重要数据,然后建立相应的数据安全保护措施和管理制度。本文件根据《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》及有关规定和标准,给出了健康医疗信息的重要数据识别和管理指南,用于指导医疗卫生健康行业领域、各地区、各部门和数据处理者开展健康医疗信息的重要数据保护工作。

健康医疗信息　重要数据识别和管理指南

1　范围

本文件规定了健康医疗信息的重要数据的定义、识别规则、识别方法，明确了健康医疗信息的重要数据识别流程及安全管理机制。

本文件适用于指导健康医疗信息的数据处理者对重要数据进行识别和安全管理，也可供卫生健康管理部门、网络安全相关主管部门以及第三方评估机构等组织开展健康医疗信息重要数据的安全监督管理与评估等工作时参考。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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 43697-2024　数据安全技术　数据分类分级规则

T/GDWJ 013-2022　广东省健康医疗数据安全分类分级管理技术规范

3　术语和定义

GB/T 25069中界定的以及下列术语和定义适用于本文件。

3.1

重要数据　key data

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。

[来源：GB/T 43697—2024，定义3.2]

3.2

个人信息　personal information

以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

[来源：GB/T 43697—2024，定义3.5]

3.3

敏感个人信息　sensitive personal information

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个人信息。

[来源：GB/T 43697—2024，定义3.6]

3.4

个人健康医疗信息 personal health medical information

能够单独或者与其他信息结合识别特定自然人或者反映特定自然人生理或心理健康相关信息，涉及个人过去、现在或将来的身体或精神健康状况、接受的医疗保健服务和与医疗保健服务相关的支付信息等。

3.5

健康医疗信息 health medical information

包括个人健康医疗信息以及由个人健康医疗信息加工处理之后得到的健康医疗相关信息。

示例： 经过对群体健康医疗数据处理后得到的群体总体分析结果、趋势预测、疾病防治统计数据等。

4 重要数据识别原则

识别健康医疗信息的重要数据宜遵循以下原则：

a) 聚焦安全影响：从国家安全、经济运行、社会稳定、公共健康和安全等角度识别重要数据；
注： 只对组织自身而言重要或敏感的数据不属于重要数据，如卫生健康行业相关机构内部管理相关数据。

b) 促进数据流动：明确安全保护重点和监管对象，防止泛化保护，促进重要数据在满足安全保护要求前提下依法进行开发利用和安全有序流动；

c) 衔接既有规定：在识别重要数据时应与卫生健康主管部门现有数据管理政策和标准规范紧密衔接；

d) 综合考虑风险：根据数据用途、面临威胁等不同因素，综合考虑数据遭到篡改、破坏、泄露或者非法获取、非法利用等风险，从保密性、完整性、可用性、真实性、准确性等多个角度识别数据的重要性；

e) 定量定性结合：以定量与定性相结合的方式识别重要数据，根据具体数据类型、特性不同采取定量或定性方法；

f) 动态识别复查：随着数据用途、共享方式、敏感性等发生变化，动态识别重要数据，并定期核查重要数据识别结果；

g) T/GDWJ 013—2022 中四级数据中的个人生物识别信息比照重要数据管理；

h) T/GDWJ 013—2022 中四级数据中的个人健康状况数据和门（急）诊病历数据超过 100 万条规模的比照重要数据管理。

i) 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：

1) 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；

2) 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；

3) 经评估的其他数据。

5 重要数据特征

健康医疗信息重要数据特征主要包括以下几方面。

a) 涉及人类遗传信息。基因数据、遗传资源等属于重要数据。包括生命登记信息、人类遗传资源信息、基因测序原始数据，以及人体基因组、基因等遗传物质的器官、组织、细胞等遗传材料的情况等。

b） 涉及健康医疗。包括：

1） 诊疗与健康管理信息。能够反映群体生理、心理特征或区域生态、生活情况，具有战略意义或可能产生重大政治、社会影响的诊疗与健康管理数据，以及批量健康医疗数据挖掘、群体画像、开发利用结果数据，属于重要数据。

2） 突发公共卫生事件相关信息。突发公共卫生事件与传染病疫情监测过程中获得的疫病流行情况，疫情防控过程中获得的病源跟踪、物资调配、交通运输等相关信息，属于重要数据，已公开的除外。

c） 涉及药品（物）和医疗器械。包括：

1） 药品（物）实验数据。国家战略安全的药品在药品审批过程中提交的药物实验数据属于重要数据。如：在药品（物）不良反应报告和监测过程中获取的患者和报告者信息；在动物模型上进行的药理、毒理、稳定性、药代动力学等试验数据，在人体中进行的临床试验数据，以及与药品的生产流程、生产设施有关的试验数据。

2） 医疗器械实验数据。《医疗器械分类规则》所定义的第二类、第三类医疗器械临床试验数据/报告属于重要数据。

3） 药品安全数据。药品溯源标识信息，包括追溯编码、产品名称、执行标准、配料、生产工艺、标签标识等，属于重要数据。

4） 药品安全重大（紧急）事件信息。非公开的药品安全重大（紧急）事件信息属于重要数据。

6 重要数据识别工作流程

6.1 数据分类分级

卫生健康相关机构依据T/GDWJ 013—2022，全面梳理机构数据资源，完成数据分类分级识别与标识工作，在此基础上实施重要数据判定工作。

6.2 重要数据判定

根据数据分类分级识别与标识的结果，重点针对安全级别较高（如依据T/GDWJ 013—2022判定为四级和三级）的数据对象，依据重要数据识别特征，逐条对数据对象进行重要数据判定工作。过程如下：

a） 梳理数据资产：对本组织内的数据资产进行盘点、梳理与分类，形成本组织数据资产清单；

b） 判断安全影响：明确资产清单中各类数据的用途、面临的主要安全威胁，判断数据安全性（保密性、完整性、可用性等）遭破坏后可能对国家安全、经济运行、社会秩序、公共利益等造成的影响，数据级别确定可参照 GB/T 43697—2024 ，6.5 相关规定，规则参见表 1；

表 1 数据级别确定规则表

影响对象	影响程度		
	特别严重危害	严重危害	一般危害
国家安全	核心数据	核心数据	重要数据
经济运行	核心数据	重要数据	一般数据
社会秩序	核心数据	重要数据	一般数据
公共利益	核心数据	重要数据	一般数据
组织权益、个人权益	一般数据	一般数据	一般数据
注：如果影响大规模的个人或组织权益，影响对象可能不只包括个人权益或组织权益，也可能对国家安全、经济运行、社会秩序或公共利益造成影响。			

c） 识别重要数据：根据所在地区、部门的具体规定，初步判定本组织数据资产中的重要数据。必要时，可使用自动化技术工具分析结构化数据、半结构化数据及非结构化数据，根据数据规模量级、关键字段、关联规律等识别其中包含的重要数据；

d） 审核重要数据：对初步识别出的重要数据进行审核；

e） 形成目录：填表描述经审核确定的本组织重要数据，以目录形式形成本组织重要数据最终识别结果。

6.3 重要数据标识

对判定为重要数据的数据对象，除分类分级标识外，增加重要数据标识。

6.4 重要数据目录

卫生健康行业各机构完成重要数据识别后，应形成重要数据目录。重要数据目录内容至少包括数据类型、内容描述、数据量、保存位置、保存期限、数据处理情况（数据处理目的、数据处理所涉及的信息系统）、数据对外提供情况（共享转让、公开披露、数据出境）、数据生命周期各环节安全措施配套情况。

附录A给出了重要数据目录示例。

7 重要数据管理

7.1 安全保护措施

除满足T/GDWJ 013—2022外，健康医疗重要数据保护可以采取的安全措施如下：

a） 指定重要数据安全管理责任机构和负责人，落实重要数据安全保护责任；

b） 对重要数据进行标识，制定统一的重要数据安全策略，加强重要数据的安全管理；

c） 建立重要数据安全管理平台，实现重要数据的统一登记、管理、检测和预警等集中管理技术机制；

d) 对重要数据的采集/收集遵从合法、正当、必要等最小化原则；采集/收集过程中对数据源进行真实性校验，传输过程中采取加密、完整性保护等安全措施，防止重要数据被篡改、窃取、损毁；
e) 对重要数据的存储采用加密、备份、访问控制、安全审计等安全措施，保障重要数据存储安全；
f) 对重要数据的使用建立严格的审批流程，确保重要数据在国家法律法规要求允许范围内使用，不影响国家安全、社会公共利益，使用过程中应当采取访问控制、脱敏、异常行为监测、接口监控、安全审计等安全措施，防止重要数据被窃取、滥用；
g) 对重要数据的采集/收集、保存、使用、对外提供等全过程进行日志记录并至少保存一年，对外提供环节日志记录至少保留两年，并采取备份、防篡改等措施保障日志数据的安全；
h) 对重要数据的采集/收集、保存、使用、对外提供等全过程进行实时安全审计；
i) 对重要数据的销毁设置安全策略和方法，严格按照策略执行审批、销毁、记录、检验等操作，并做好相关介质的管理和销毁。

7.2 安全评估管理

除满足T/GDWJ 013—2022相关要求外，健康医疗信息重要数据安全评估机制应包括：

a) 至少每半年对重要数据收集使用情况进行一次安全评估；
b) 对外提供、公开发布重要数据前，应开展安全评估；健康医疗信息重要数据应在境内存储，确需出境的，出境前应开展安全评估；
c) 安全评估报告应包括重要数据的种类、数量，收集、存储、加工、使用数据的情况，面临的数据安全风险及其应对措施等。

7.3 安全事件管理

健康医疗数据处理者应制定切实可行的数据安全应急预案，建立相应应急机制，定期开展应急演练，采取必要措施消除安全隐患。发生重要数据泄露、损毁、丢失等安全事件，或者发生数据安全事件风险明显加大时，健康医疗数据处理者应当立即采取补救措施和记录处置过程，并及时按要求向上级主管部门上报。

附 录 A
（资料性）
健康医疗信息重要数据目录示例

重要数据梳理识别情况汇总表

序号	数据基本情况													责任主体情况							数据处理情况						数据安全情况								是否建议纳入核心数据目录*	备注
	数据名称*	依据数据分类分级规范*	数据一级分类*	数据二级分类*	数据三级分类*	数据四级分类*	数据级别*	数据载体*	数据来源*	数据量(GB)*	数据量(条)*	数据覆盖情况		数据精度	数据处理者名称*	机构代码*	数据处理者所在地		数据安全负责人			数据处理目的*	数据出境情况			是否涉及跨主体流动*	是否为涉外数据*	信息系统名称及IP地址*	网络安全等级保护情况*	是否为关键信息基设*	数据安全风险评估情况						
												覆盖类型*	覆盖占比*				省*	市*	姓名*	职务*	联系方式*		是否出境*	是否开展数据出境安全评估*	数据出境安全评估结果						是否进行数据安全风险评估*	评估机构	评估规范	评估时间	评估结论		
示例	门诊电子病历数据	T/GDWJ 013-2022 广东省…规范	业务资源类	医疗服务	临床服务		重要数据	连接互联网系统	自动采集	5648 1	1048 000	领域	超过80%		XX XX医院	91…324	广东省	东莞市			152…X	XXXX	是	是	XXXX	是	是	A业务系统 10.*.100.22	三级	是	是	双*	(XXX规范)	2022年9月	XXXX	是	
1																																				
2																																				

填报说明：标*的字段为必填项，数据分类“一级、二级、三级、四级内容”,具体参考《WS/T 787—2021 国家卫生信息资源分类与编码管理规范》。

参 考 文 献

[1] GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型
[2] GB/T 39725-2020 信息安全技术 健康医疗数据安全指南
[3] GB/T 41479-2022 信息安全技术 网络数据处理安全要求
[4] JR/T 0197-2020 金融数据安全 数据安全分级指南
[5] YD/T 3867-2021 基础电信企业重要数据识别指南
[6] 卫生健康行业数据分类分级指南（试行）
[7] 信息安全技术 重要数据处理安全要求（征求意见稿，2023 年 8 月 10 日）