ICS 35.030
CCS L 70

DB3203

徐 州 市 地 方 标 准

DB XX/T XXXX—XXXX

医疗机构视频数据安全建设规范

Specification for video data security construction in medical institutions

2024－XX－XX 发布　　2024－XX－XX 实施

徐州市市场监督管理局　　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。

本文件由徐州市卫生健康委员会提出并归口。

本文件起草单位：徐州市公安局、徐州网络公共安防技术协会、徐州医科大学、南京医科大学、慧盾信息安全科技（苏州）股份有限公司、徐州医科大学附属医院、沛县人民医院、徐州市中心医院、徐州市东方人民医院、陆军第七十一集团军总医院。

本文件主要起草人：吴响、卜庆亚、李同武、王换换、夏有兵、吴保鑫、张敬涛、史志强、周泽军、权维、郑海源、陆江涛、蔡成明、谈永奇。

引　言

随着新一代信息技术的快速发展，互联网医院、智慧医疗、远程医疗、远程示教等新型医疗业务蓬勃发展，其中医疗视频数据的采集、传输、共享和挖掘应用等成为支撑新型医疗业务发展运行的关键。同时，随着人工智能、大数据、物联网等技术在医疗信息行业中的推广应用，基因、人脸、指纹、手术、视网膜等新型数据也将成为医疗机构视频数据的重要组成部分。而此类视频数据具备人体可唯一标识属性，涵盖大量个体隐私信息，为更好地保护医疗机构视频数据，规范和推动医疗机构视频数据的开放共享和挖掘应用，促进医疗信息行业快速、高质量发展，特制定医疗机构视频数据安全建设规范。

国家先后颁布和实施了《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》，均指明了数据保护工作方向，明确了数据安全主管机构的监管责任，目前已初步形成了数据安全战略布局。2022年8月，国家卫健委、国家中医药局、国家疾控局三部门联合制定并颁布了《医疗卫生机构网络安全管理办法》，明确提出了相关监管单位对于医疗卫生机构网络数据安全管理的总体要求。

本文件为医疗机构视频数据的安全管理提供更加精细化的建设规范，为整体提升医疗机构视频数据安全管理能力与建设规范性提供科学、可操作性的安全建设思路、技术应用规范、设备检验方案支持以及视频数据安全建设案例参考。

医疗机构视频数据安全建设规范

1 范围

本文件规定了医疗机构视频数据安全建设的目标、分类分级，采集、存储、处理、应用及销毁的管理要求。

本文件适用于徐州市行政区域范围内医疗机构视频数据的安全建设工作。

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 37740 信息技术 云计算 云平台间应用和数据迁移指南

GB/T 37964-2019 信息安全技术 个人信息去标识化指南

GB/T 37973-2019 信息安全技术 大数据安全管理指南

GB/T 39205 信息安全技术 轻量级鉴别与访问控制机制

3 术语和定义

GB/T 25069-2022、GB/T 35273-2020、GB/T 37964-2019界定的以及下列术语和定义适用于本文件。

3.1

医疗机构视频数据 video data from medical institutions

医疗机构在日常医疗服务、管理及相关活动过程中，通过各种视频采集设备所获取、存储和处理的以视频形式存在的或通过专业影像设备生成的动态视频数据的信息集合。

3.2

访问控制 access control

一种确保数据处理系统的资源只能由经授权实体以授权方式进行访问的手段。

[来源：GB/T 25069-2022, 3.147]

3.3

去标识化 de-identification

通过对个人信息的技术处理，使其在不借助额外信息的情况下，无法识别个人信息主体的过程。

[来源：GB/T 35273-2020, 3.15]

3.4

重标识 re-identification

把去标识化的数据集重新关联到原始个人信息主体或一组个人信息主体的过程。

[来源：GB/T 37964-2019, 3.9]

3.5

数据管理中心 data resource center

对各类数据进行集中存储、管理、处理和共享，提供数据支持与服务的综合性平台。

4 建设目标

医疗机构应在实现视频数据价值的同时，采取合理、适当且安全的建设方案与技术保障措施，以达到以下安全建设目标：

a）确保医疗机构视频数据的保密性、完整性与可用性；

b）确保医疗机构视频数据使用和公开过程的合法合规性，保护患者个人隐私信息安全、社会大众利益以及国家安全；

c）确保医疗机构视频数据在符合上述安全建设规范和目标要求的基础上，满足现代信息化医疗业务正常开展需求。

5 分类分级

5.1 原则

医疗机构应坚持科学性、稳定性、实用性和扩展性相统一的原则完成医疗机构视频数据的分类分级工作。应建立视频数据分类分级动态调整机制，每年定期评估，依据数据价值、敏感程度变化及法规政策调整进行分类分级，确保数据管理科学合理。

5.2 类别

根据医疗机构视频数据产生的场景（见GB/T 39725-2020 6.1），将医疗机构视频数据划分为以下4个类别：

a）医疗诊断与治疗类：包括但不限于影像诊断视频，借助 X光、CT、MRI、超声等专业影像设备，在检查期间所生成的动态视频数据；内镜诊疗视频，包含胃镜、肠镜、支气管镜等内镜检查全程记录的视频数据；手术全程视频：完整且详细地记录手术从开始到结束的整个过程，其中涵盖手术切口的位置与方式、具体的操作步骤以及对组织器官的处理细节等视频数据。

b）医疗护理与康复类：包括但不限于护理操作视频，记录护士在执行静脉穿刺、换药、导尿等日常护理操作过程的视频数据；康复训练视频，精准记录康复患者在进行肢体运动、语言功能、认知能力等康复训练过程的视频数据。

c）医疗管理与监控类：包括但不限于病房监控视频，在病房区域安装监控设备所获取的视频数据，对于重症患者、昏迷患者以及特殊患者等，记录患者的病情变化、活动情况以及病房内的安全状况；医疗设备监控视频，针对重症监护室中的生命支持设备、放疗设备等大型关键医疗设备运行状态进行实时监控所产生的视频数据；公共区域监控视频，分布在医院大厅、走廊、电梯间、停车场等公共区域的监控设备所采集的视频数据。

d）医疗教学与科研类：包括但不限于教学示范视频，由经验丰富的资深医生或专业教师进行临床操作示范、典型病例讲解等过程所录制的视频数据；科研观察视频，在医学科研项目实施过程中，对实验的具体过程、研究对象的相关情况进行详细记录所形成的视频数据。

5.3 级别

根据医疗机构视频数据的重要价值与保密级别（见 GB/T 22240-2020 4.1、GB/T 39725-2020 6.2 以及 GB/T 35273-2020 附录 A 和附录 B），将医疗机构视频数据划分为以下 5 个级别：

a）第1级：可完全公开使用的数据。不涉及任何敏感信息，如医疗机构的宣传视频、普及医学常识的视频数据等。此类数据可直接在互联网以及微信群、微博、公众号等社交平台公开。

b）第2级：可在较大范围内供访问和使用的视频数据。数据无法通过任何方式关联到特定个人，且具有一定医学科学研究价值。此类数据经过申请与审批可用于医学科学研究与分析。

c）第3级：可在中等范围内供访问使用的视频数据。数据经过去标识化处理，仍存在被重标识的风险，如未经授权披露，可能会对视频数据主体造成伤害。此类数据仅限于获得授权的项目组范围内使用。

d）第4级：可在较小范围内供访问和使用的视频数据。包含可以识别特定自然人的视频数据，如生物信息识别、疾病诊断等内容。如未经授权披露，可能会对视频数据主体造成较大伤害。此类数据仅限于相关科室部分医护人员访问和使用。

e）第5级：可在极小范围内供访问和使用的视频数据。涉及重大公共卫生事件、特殊病种诊断以及人类遗传资源的视频记录和影像数据，具有极高的敏感性和重要性。此类数据仅限于疾控中心相关人员、主治医师及部分科研人员访问，且需要进行严格管控。

6 采集管理要求

6.1 采集范围和对象

确定视频数据的使用场景、人员或机构，明确视频数据的采集范围和对象，包括医疗诊断与治疗类、医疗护理与康复类、医疗管理与监控类以及医疗教学与科研类。

6.2 采集规范

医疗机构应按照GB/T 35273-2020中5.1和5.2的要求，在遵循合规原则、质量保障原则及安全原则的基础上，遵循数据采集最小必要原则，制定采集规范，明确采集视频的分辨率、格式、帧率等，确保采集视频数据的完整性、准确性和可靠性。医疗机构宜参照GB/T 37973-2019中8.2的要求，制定具体可实施的视频数据采集流程规范，包括采集前准备、采集过程控制、采集后处理等环节，保证采集人员能够按照规定进行操作，保证视频质量与安全。

6.3 采集设备和网络

医疗机构应选择安全的视频数据采集网络和设备，包括但不限于基于虚拟专用网络技术的安全网络、带防火墙部署的硬件设备，确保用于视频数据采集的内部网络和外部网络隔离，保证视频数据能够安全、稳定地传输和存储。同时，应定期对视频采集设备和网络进行安全检查以及维护升级。

6.4 隐私性与合规性

在视频数据采集过程中应充分考虑视频主体隐私保护与合规性要求，对涉及患者隐私的视频进行去标识化与加密处理，确保患者隐私得到保护。医疗机构必须严格按照《中华人民共和国个人信息保护法》《医疗卫生机构安全管理办法》要求，确保被采集的视频数据主体的知情同意以及相关伦理委员会的审查同意。

7 存储管理要求

7.1 存储架构选择

医疗机构应结合视频数据等级、用途、规模、访问频率以及安全性要求等，分别采用安全、有效的视频存储方式与架构，如采用分布式存储、云存储、集中式存储或磁盘存储等方式，确保视频存储的高可用性、可扩展性与容错性。

7.2 加密与脱敏

医疗机构必须遵循《中华人民共和国数据安全法》，根据视频数据安全级别，采用加密、对称加密等方式，对视频数据进行加密存储管理。同时对涉及患者隐私信息的数据进行脱敏处理，保证视频主体隐私安全。

7.3 存储安全

针对医疗机构生产、运维、教学、监控中产生的敏感视频数据，应保证视频数据在存储过程中的安全；通过对数据资产识别与审计，对存储和处理数据的数据管理中心、云计算和大数据平台进行监测和防护，保障重要、敏感视频数据防删除、防损毁、防篡改，防止利用系统漏洞嗅探/攻击，全面保障视频数据安全。

7.4 审计安全

医疗机构应对用户针对视频数据的各种操作全程审计，包括但不限于：

a）建立能够监控数据管理中心多重状态与通信内容的审计系统，不仅支持对数据管理中心面临的风险进行多方位评估，还应对数据管理中心的所有操作进行审计，并提供事后追查机制；

b）应具备良好的数据管理中心兼容性，支持主流数据库系统和国产操作系统的审计，并兼容大数据平台；

c）应实时监测数据管理中心的异常访问行为，如异常 IP 访问、异常时间段访问、越权操作、删除系统级库/表等高危操作，实时预警，确保数据安全；

e）应建立具体可实施的视频数据审计管理机制，对视频数据安全存储管理过程进行实时监控和记录；

f）通过日志记录、监控告警等方式，及时发现、处理和记录异常事件，并定期检查和分析审计记录与日志，做好安全风险与漏洞的事前感知工作。

7.5 对外共享安全

医疗机构在对外单位发布或者共享视频数据时，应采用以下措施保证数据共享安全，包括但不限于：

a）应统一管理对外数据共享接口，监测对外共享数据的行为和对外共享数据的合规性，以及控制和监管对外共享的敏感数据的使用；

b）应对视频数据交换的过程、数据内容进行全面安全审计；

c）应采用嵌入数据水印技术，对交换的数据实现追溯。

7.6 运维安全

医疗机构针对视频数据进行运维时，应具备:

a）安全准入能力，包括运维终端准入、运维账户准入、以及运维工具准入；

b）数据加密能力，从运维堡垒机导出、下载的数据文件落地加密；

c）运维电脑防护能力，针对运维电脑防截屏、录屏及拍照能力，通过阻断截屏录屏操作，通过屏幕或应用水印的方式警示拍照和溯源拍照行为。

7.7 备份与恢复

医疗机构应制定安全可实施的视频数据备份与恢复方案，包括但不限于：

a）备份视频数据应存储在安全可靠的设备或云端，并采取必要的加密、访问控制与去标识化等手段，确保视频数据安全；

b）定期对采集和存储的视频数据进行备份，其中关键数据（本文件 5.3 中的第 3、4 级）应每小时备份一次，防止数据丢失；

c）重要数据（本文件 5.3 中的第 5 级）应存储 15 年～30 年，其中申请应用于科研的视频数据，在研究结束或终止后，应及时删除相关视频。

8 处理管理要求

8.1 分类与标记

医疗机构应根据视频数据的用途、敏感程度以及分类分级结果，对视频数据分别进行分类和标记，并制定明确的处理规则和安全措施，确保视频的正确处理和保护。

8.2 清洗与去标识化

医疗机构应对采集的视频数据进行清洗，按GB/T 37964的要求，建立明确的去标识化目标、原则和流程。保证在可控的环境、方式、目的、范围和期限内公开供特定组织机构、可信第三方和个人共享。其中去标识化目标、原则、流程及策略应由视频数据安全管理团队审批。视频数据实际应用时，相关去标识化要求如下：

a）统一要求。去除视频数据中可唯一识别特定自然人的非研究和教学用生物信息，如身份信息、人脸信息、指纹等，自然人包括医生、护士、患者等。

b）应用于医学教育。去除视频中可唯一识别特定自然人的非教学用生物识别信息，例如身份信息、面部特征、指纹、虹膜、耳廓、声纹等，仅保留教学用关键视频信息。

c）应用于临床研究。仅保留视频中与临床研究相关的关键信息，并去除可唯一识别特定自然人的生物识别信息。

d）应用于医学新技术研究。疾病视频、影像文件保留用于医学新技术研究所必需的关键疾病特征，去除可唯一识别特定自然人的生物识别信息，并阻断重标识化。

e）应用于智能辅助诊断。首先进行去标识化处理，用于开展远程或在线智能辅助诊断，在需要进行重标识确定主体时，应由医疗机构或相关部门专人处理，处理过程严格保密。

f）视频使用者不得参与去标识化相关工作。

g）在视频控制者可控公开共享模式下，视频使用者应签署视频使用协议，保证视频使用全流程安全，并及时记录视频使用情况，接受视频控制者安全审计。

8.3 迁移与归档

医疗机构应根据实际需求和视频数据生命周期管理要求，宜按照GB/T 37740的要求，对视频数据进行迁移和归档，并做到：

a）应确保数据的安全性和完整性；

b）应进行视频数据去隐私和脱敏处理，并确保视频数据的可追溯性与可审计性。

8.4 监控与审计

医疗机构应建立明确、可实施的视频数据处理监控和审计机制，对视频数据处理过程进行实时监控和记录，通过日志记录、监控告警等方式，及时发现和处理异常事件。应对审计记录进行定期检查和分析，以便及时发现潜在的安全风险和漏洞，确保视频数据处理全程可追溯。

8.5 应急预案与处置

医疗机构应结合视频数据处理要求制定应急预案，对可能出现的意外情况进行及时响应和处理。同时应明确应急处置流程、具体责任人等，确保在发生紧急情况时能够迅速采取有效措施。

9 应用管理要求

9.1 应用场景划分

医疗机构作为视频数据的控制者，应明确视频数据的使用场景，具体包括医学影像诊断、手术监控、住院患者监控、医学教育培训以及医学科学研究等。根据不同应用场景，医疗机构应联合相关单位，包括但不限于：伦理审查委员会、地方卫健委等，制定相应的视频数据安全策略与使用规范，做到以下几点：

a）医疗诊断与治疗监控场景中，未经授权不得访问影像视频数据，影像传输采用专用加密通道，存储时加密处理且定期备份，确保数据不泄露、不丢失；严格限制手术室监控视频的访问权限，仅手术团队成员、医疗质量监管人员在特定手术期间及后续质量评估时可查看；监控视频实时加密传输，存储采用高安全性存储设备并进行多重加密；

b）医疗护理与康复监控场景中，应严格依据患者的授权范围（如患者主管医护人员等）使用数据，不得超范围使用；未经患者再次同意，不得将数据用于其他用途；当涉及多部门或多人协作使用数据时，需建立规范的协作流程，明确数据传递方式和各方责任，确保数据在协作过程中的安全。

c）医疗管理监控场景下，限制访问权限为患者主管医护人员、病房值班人员等。监控数据存储在医院内部安全区域，定期清理超过一定期限（如三个月）的普通监控数据，但涉及医疗纠纷、特殊病情等数据长期保存；

d）医疗教学与科研场景中，明确可访问视频数据的学员范围，对用于教学的视频进行去标识化处理，去除可识别患者身份的敏感信息；严格管控视频的传播范围，学员仅能在指定教学场所使用，不得私自传播、拷贝；研究人员获取视频数据需经严格审批流程，审批通过后按最小授权原则分配访问权限。对用于研究的视频数据进行严格去标识化处理，防止研究过程中泄露患者隐私。研究结束后，及时删除不再使用的数据，并对删除过程进行记录和审计。

9.2 访问控制和权限管理

医疗机构应按照GB/T 39205的要求，根据视频数据的安全级别以及相关用户角色划分，建立明确的视频访问控制和权限管理制度。针对不同用户，医疗机构应设定不同的访问权限和操作权限，并根据用户的岗位职责和工作需求，分配相应的访问和操作权限。可信第三方获取和使用视频数据时，也应遵守相关规则和要求，确保数据的安全性与保密性。

9.3 使用合规性审查

医疗机构应定期对视频数据的使用进行合规性审查，保证视频数据仅用于申请使用的最小范围内，并确保视频数据的使用合法、合规。合规性审查内容包括但不限于视频数据采集、存储、处理、使用和发布等环节，确保符合相关法律法规和伦理要求。视频数据使用合规性审查由医疗机构内部的相关部门

共同执行，审查视频数据使用过程中的技术安全合规性，确保数据访问、存储、传输等环节符合信息安全相关标准和规范。

9.4 隐私防护

在视频数据应用过程中，医疗机构应按照本文件8.2的要求，采取去隐私、匿名化等处理方式，确保视频数据主体隐私安全，防止个人隐私信息泄露和滥用。

9.5 监督和审查

对于无法继续完成或已经完成的相关研究，医疗机构应及时告知视频数据使用者删除相关数据，并确保不可恢复。

10 销毁管理要求

10.1 销毁政策制度

医疗机构应制定明确的视频数据销毁制度，规定视频数据的销毁范围、销毁方式、销毁时间和责任人等。应按照规定时间间隔对视频数据进行销毁，并及时记录视频数据的销毁过程，保证视频数据销毁流程的可追溯和验证过程的有效性。

10.2 物理销毁

对于不可恢复的视频数据，医疗机构宜采用物理销毁的方式，如粉碎、焚烧等，确保视频无法被还原。在物理销毁过程中，应注意操作的安全性和环保要求，避免对环境和人员造成损害。

10.3 逻辑销毁

对于可恢复的视频数据，医疗机构宜采用逻辑销毁的方式，如覆写、加密等，使视频数据无法被读取或解密。同时，逻辑销毁应采用可靠有效的技术手段，确保数据无法被恢复或破解。

10.4 第三方验证

为确保使用逻辑销毁的视频数据被彻底销毁，医疗机构可通过第三方机构进行验证，通过技术手段对销毁过程进行监测和验证，确保视频数据已被彻底销毁。

10.5 存储介质安全处理

对于存储视频数据的介质，包括但不限于硬盘、光盘、U 盘等，在销毁前应进行安全处理，可以采用物理破坏和化学腐蚀等方式，确保存储介质中的视频数据无法被读取或恢复。

参 考 文 献

[1] GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南

[2] GB/T 39725-2020 信息安全技术 健康医疗数据安全指南

[3] 中华人民共和国数据安全法（中华人民共和国主席令第 84 号）

[4] 中华人民共和国个人信息保护法（中华人民共和国主席令第 91 号）

[5] 医疗卫生机构网络安全管理办法（国家卫健委、国家中医药局、国家疾控局）