ICS 01.100.01
CCS J 04

团 体 标 准

T/SCGS 313008—2024

隐私增强的医学影像数据管理规范

Data management specifications of medical imaging for privacy-enhanced

全国团体标准信息平台

2024-04-16 发布　　2024-04-17 实施

中国图学学会　发布
中国标准出版社　出版

目　　次

全国团体标准信息平台
中国标准出版社

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。

请注意本文件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。

本文件由中国图学学会提出并归口。

本文件起草单位：中国科学院自动化研究所、澳门城市大学、北京航空航天大学、广东省人民医院、珠海市人民医院、河南省人民医院、北京大学人民医院、北京大学第三医院。

本文件主要起草人：刘西蒙、刘振宇、应作斌、刘建刚、刘再毅、陆骊工、王梅云、王姝、卢剑、蔡剑平、刘明昊、方一晨、张国扬。

全国团体标准信息平台
中国标准出版社

隐私增强的医学影像数据管理规范

1 范围

本文件规定了医学影像数据的隐私管理、医学影像数据的联合建模流程要求。

本文件适用于医学影像数据联合建模过程中的数据管理，包括采集、脱敏、传输等过程。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1 数据管理领域

3.1.1

隐私增强 privacy-enhanced

保护敏感信息隐私或机密性的技术方法。包括在隐私信息采集、存储，以及在执行搜索或分析过程中对于保护和增强隐私安全性的数据安全技术。

注：旨在遵守隐私和数据保护原则，同时保持从用户提供的数据中提取价值的能力。

[ISO/IEC 20889:2018，3.3，有修改]

3.1.2

数据采集 data acquisition

从传感器和其他待测设备等模拟和数字被测单元中自动采集非电量或者电量信号，送到计算机中进行分析、处理。

[T/CESA 1049—2018，6.2，有修改]

3.1.3

数据泄露 data breach

将机密信息、私人信息或其他敏感信息发布到不安全的环境中。

注：数据泄露可能由意外引起，也可能是蓄意攻击的结果。

[T/CESA 1049—2018，6.5，有修改]

3.1.4

数据传输 data transmission

按照一定的规程，通过一条或者多条数据链路，将数据从数据源传输到数据终端。

注：它的主要作用是实现点与点之间的信息传输与交换。

3.1.5

数据加密 data encryption

将一个信息经过加密钥匙及加密函数转换，变成无意义的密文，而接收方则将此密文经过解密函

数、解密钥匙还原成明文的手段。

[T/CESA 1049—2018,6.4,有修改]

3.1.6

数据存储　data storage

使用计算机或其他设备通过记录介质来保存数据,它是一种采用专门开发技术的信息保留方式,能够保存相应数据并确保可在需要时对其进行访问。

注:最常用的数据存储方式有文件存储、块存储和对象存储,每种存储方式都有不同的用途。

[T/CESA 1049—2018,6.3,有修改]

3.1.7

数据分类　data classification

根据组织数据的属性或特征,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组织数据的过程。

3.1.8

数据归档　data archiving

将不再经常使用的数据移到一个单独的存储设备来进行长期保存的过程。

3.1.9

数据销毁　data destruction

计算机或设备在弃置、转售或捐赠前必须将其所有数据彻底删除,并无法复原,以免造成信息泄露,尤其是国家级的涉密数据。

3.2　医学领域

3.2.1

医学影像　medical imaging

利用医学成像设备及技术所得到的图像。

[T/NAHIEM 47—2022,3.1]

3.2.2

磁共振成像　magnetic resonance imaging

一种医学成像技术,利用磁场和计算机生成的无线电波来创建人体器官和组织的详细图像。

3.2.3

计算机断层扫描　computed tomography

计算机断层扫描组合了一系列从身体周围不同角度拍摄的 X 光图像,并运用计算机进行处理,以创建体内骨骼、血管和软组织的横截面图像(切片)。

[T/CESA 1109—2020,7.4,有修改]

3.2.4

X 光　X-ray

一种波长范围在 0.01 nm～10 nm 之间的电磁辐射。

3.2.5

超声成像　ultrasound imaging

利用超声声束扫描人体,通过对反射信号的接收、处理,以获得体内器官的图像。

[T/CESA 1109—2020,7.1,有修改]

3.2.6

核医学　nuclear medicine

分子影像学的组成部分，因为其产生的是那些反应性细胞和亚细胞水平上所发生的生物学过程的图像。

[T/CESA 1109—2020，7.6，有修改]

3.2.7

功能性磁共振成像　functional magnetic resonance imaging

一种神经影像学技术。

注：原理是利用磁振造影来测量神经元活动所引发的血液动力改变。

3.2.8

微波成像　microwave imaging

以微波作为信息载体的一种成像手段，实质属于电磁逆散射问题。

注：既用它的幅度信息，也用它的相位信息。

4　缩略语

下列缩略语适用于本文件。

CT：计算机断层扫描(computed tomography)

DU：多普勒成像(duplex ultrasound)

EIT：阻抗成像(electrical impedance tomography)

FMRI：功能性磁共振成像(functional magnetic resonance imaging)

MI：微波成像(microwave imaging)

MRI：磁共振成像(magnetic resonance imaging)

NM：核医学(nuclear medicine)

UI：超声成像(ultrasound imaging)

X-ray：X 光(roentgen ray)

5　隐私增强的医学影像数据管理规范

5.1　数据采集

5.1.1　通用要求

应按照最小必要等原则采集外部医学影像数据，明确医学影像数据目的和用途的真实有效，保证医学影像数据采集的合法性、合规性、正当性。

5.1.2　数据采集

数据采集要求如下：

a）　应明确医学影像数据采集安全管理要求，包括组织采集医学影像数据时的原则，医学影像数据的直接或间接采集流程和方法；

b）　应明确医学影像数据已获得患者个人信息处理的授权同意范围，包括使用目的、采集范围、患者是否授权同意共享等；

c）　应根据患者个人的诊断情况，有选择地采取数张不同类型的医学影像数据；

d） 应规定医学影像数据采集的渠道，并对采集来源方式、数据范围和类型进行记录，确保不收集、不提供与服务无关的个人信息；

e） 应采取相应的技术手段，确保采集过程中的患者个人信息不被泄露，尤其是个人敏感信息数据，个人敏感信息包括但不限于标识个人身份的医学影像数据、特殊病种的详细影像资料。

5.1.3 数据分类

应按照属性或特征对数据进行归集分类，以满足数据建模及应用管理中对数据进行查询、识别、管理、保护和使用需求。医学影像数据分类见表1。

表1 医学影像数据分类表

数据类别		范围
个人生物识别影像数据		基因、指纹、声纹、掌纹、耳廓、虹膜、面部特征等
临床影像数据	结构图像：描述人体的生理解剖结构	X光（X-ray）、计算机断层扫描（CT）、超声成像（UI）、磁共振成像（MRI）
	功能图像：描述人体在不同状态下组织器官的功能活动状况	核医学（NM）成像、功能性磁共振成像（FMRI）、多普勒成像（DU）
	其他类型成像	阻抗成像（EIT）、微波成像（MI）、光学成像

5.2 数据脱敏

各医疗机构在设定具体场景下数据脱敏策略时，应充分考虑数据脱敏后数据可用性及数据保密性，寻求两者间的平衡。选择数据脱敏策略见表2。

表2 数据脱敏策略表

数据可用性	数据保密性	
	高	低
高	宜使用：同态加密 不宜使用：遮挡、替代	宜使用：泛化技术、随机干扰、重排、置换、屏蔽、替代 不宜使用：数值变换、空值插入
低	宜使用：对称加密算法（AES、SM1、SM4）、替代、空值插入、数据变换 不宜使用：遮挡	宜使用：统计技术、随机化技术、泛化技术、数据截断、空值插入、遮挡 不宜使用：加密技术
注：数据可用性“高”即脱敏后数据满足应用要求且数据失真程度较低；数据可用性“低”即脱敏后数据满足应用要求且数据失真程度较高。数据保密性定级为“低”指医学影像数据泄露无法对特定的主体的个人隐私与人格尊严造成实际损害或威胁；数据保密性定级为“高”指医学影像数据泄露造成事情（事故）的影响结果为“情节严重”或“情节特别严重”。有关具体数据类型与脱敏关系的策略当具体问题具体分析。		

5.3 数据传输

5.3.1 通用要求

根据数据传输的不同需求，应建立不同的数据加密保护策略和安全防护措施，防止传输过程中的数

据泄露。

5.3.2 数据传输要求

数据传输要求如下：

a) 明确数据传输前的安全管理要求，数据管理员与数据研究者签署数据使用协议，约定双方权责，包括数据使用者对数据的使用途径、使用期限、对数据的保护措施、数据泄露的应急方案等；

b) 在数据分类分级定义的基础上制定数据传输安全管理要求，明确不同场景下的数据传输安全要求，如：传输通道加密、数据内容加密、签名验证、身份鉴别等；

c) 建立数据传输接口安全管理工作要求，包括安全域内、安全域间等数据传输接口要求。

5.4 数据存储

5.4.1 通用要求

根据数据存储介质的访问和使用场景，以及业务特性和数据存储安全要求，应采取有效的技术和管理手段，实现对数据逻辑存储、存储容器的有效安全控制，按附录 A。

5.4.2 数据存储要求

数据存储要求如下：

a) 建立管理存储介质和逻辑存储所需要遵循的安全管理制度体系，包括安全管理政策、实施细则及指导方案；

b) 通过密码技术等方式实施完整性控制，确保医学影像数据是准确的、完整的，并为其提供应对非法修改的保护机制；

c) 制定数据备份及恢复策略，定期进行数据备份，建立介质存取、验证和转储管理制度；

d) 建立基于主体角色授权的访问控制，并在此基础上建立基于客体属性授权的访问控制。针对个人信息、敏感数据、重要数据的访问建立零信任保护机制，实现权限的动态访问控制。

5.5 数据分类

根据数据重要程度、风险级别以及对医学影像数据主体可能造成的损害和影响的级别进行分类，应将医学影像数据划分为以下 5 级。

第 1 级：可完全公开使用的数据。包括可以通过公开途径获取的数据，可直接在互联网上面向公众公开。

第 2 级：可在较大范围内供访问者使用的数据，涉及千级别数据处理，包括不能标识个人身份的数据，各科室医生经过申请审批可以用于研究分析。

第 3 级：可在中等范围内供访问使用的数据，涉及万级别数据处理。如果未经授权披露，可能对医学影像数据主体造成中等程度的损害，包括经过部分去标识化处理，但仍可能重新标识的数据，仅限于获得授权的项目组范围内使用。

第 4 级：在较小范围内供访问使用的数据，涉及百万级别数据处理。如果未经授权披露，可能对医学影像数据主体造成较高程度的损害，包括可以直接标识个人身份的数据，仅限于参与诊疗活动的医护人员访问使用。

第 5 级：仅在极小范围内且在严格限制条件下供访问使用的数据，涉及千万级别数据处理。如果未经授权披露，可能对医学影像数据主体造成严重程度的损害，包括特殊病种的详细影像资料，仅限于主治医护人员访问且需要进行严格管控。

5.6 数据使用

5.6.1 通用要求

根据医学影像数据分析，数据挖掘过程面临的安全风险，建立有效的安全管控措施，防止数据泄露。

5.6.2 数据使用要求

数据使用要求如下：

a) 建立数据权限申请审核流程，对数据源、数据使用场景、数据使用范围、数据使用逻辑、个人信息安全影响情况进行审核，以确保数据使用的真实性、必要性、合规性；
b) 制定数据使用要求，明确数据的使用范围和权限、合规要求、数据使用限制、使用安全防护要求，包括但不限于数据脱敏、访问控制；
c) 建立数据访问和授权机制。建立完善的身份认证以及基于角色的权限控制，严格区分不同用户角色对数据访问的权限。合理、精细地定义角色权限，避免不必要的，超过角色合法职责之外的授权；
d) 对数据的使用活动进行审计，重点对医学影像数据的访问以及操作的合规性进行审计，确定必要的审计控制范围和需要审计的数据。

5.7 数据归档

数据归档的要求包括但不限于：

a) 根据不同阶段的医学影像数据，建立数据归档过程中不同的安全策略和管控措施，防止数据泄露；
b) 根据医学影像数据生命周期和业务要求，建立不同阶段医学影像数据归档存储相关的操作规程；
c) 建立归档医学影像数据的安全策略和管控措施，确保非授权用户不能访问归档医学影像数据；
d) 建立归档医学影像数据的压缩或加密策略，确保归档医学影像数据存储空间的有效利用和安全访问。

5.8 数据销毁

数据销毁的要求包括但不限于：

a) 通过制定数据销毁机制，实现有效的数据删除管理。防止因对存储介质中的数据进行恢复而导致的数据泄露风险；
b) 建立医学影像数据销毁策略、管理制度和审批制度，明确销毁对象和流程；
c) 依照医学影像数据分级分类，建立相应的数据销毁机制，明确销毁方式和销毁要求；
d) 针对网络存储医学影像数据，采取硬销毁和软销毁的数据销毁方法和技术。如：基于安全策略、基于分布式杂凑算法等网络数据分布式存储的销毁策略与机制；
e) 针对闪存、硬盘、磁带、光盘等存储数据，采取硬销毁和软销毁的数据销毁方法和技术；
f) 配置必要的医学影像数据销毁工具，确保以不可逆方式销毁医学影像数据及其副本内容。

全国团体标准信息平台 中国标准出版社

附 录 A
（规范性）
数据管理规范的解释说明

A.1 被访问的病人数据的隐私保护

A.1.1 医生分级分类

医生为病人提供医疗服务过程中会查阅病人的医学数据。此时，数据可分为默认级数据、告知级数据、授权级数据。具体要求如下：

a） 默认级数据包括检验检查名称、就诊医院、就诊科室等；

b） 告知级数据包括检验检查报告、手术记录、出院小结等；

c） 授权级数据包括住院详细病历、患病详细信息等。

A.1.2 医生角色定义

不同角色的医生的调阅权限不同，角色定义清晰，方可进行下一步的权限分配。原则上，宜按所在科室、职称、诊疗组来定义角色类型：

a） 科室即不同诊疗科室，按照医院科室划分，包括消化科、心脏外科等；

b） 职称表示医生的专业性，包括但不限于主任医师、主治医师、住院医师；

c） 诊疗组即按诊疗组划分，按照医院科室的具体划分而定，不同诊疗组之间的患者管辖相对独立，包括普外科内部分为胃肠诊疗组、肝胆诊疗组等，若科室内部未划分则无须定义。

A.1.3 医生权限分配

将医生的科室、职称、诊疗组与数据分级、颗粒度匹配。每个医生仅可调阅自身管辖范围内患者的数据，上级医师可查看下级医师管辖范围内的患者数据。权限具体要求：

a） 对于普通病种的资料，权限范围内医生均可调阅。对于特殊病种的资料，不同职称医生的权限不同；

b） 对于传染性疾病，考虑保护医务人员原则，默认向接诊医护人员披露。

A.2 患者本人查询数据的隐私保护

A.2.1 身份识别

病人进行身份识别的具体方式，以及拥有的查询权限如下：

a） 患者通过在线系统查询其健康医学数据，首次注册应通过实名认证的手机号码和手机验证码登录。账号可绑定子女手机（上传身份证或户口本扫描件即可或由系统后台认证）由监护人或授权子女代替查询信息；

b） 系统应对可查询信息进行适当限制。包括局部部位 CT 等敏感检查结果不予显示等操作；

c） 默认可查询 3 个月内相关检查检验报告、用药情况等。

A.2.2 操作权限

个人用户具体操作权限的相关信息如下：

a） 系统应合理设置个人的操作权限；

b） 操作权限包括另存、复制、打印、下载等。个人进行相应操作时，页面显示用户须知，包括告知患者下载数据后，患者本人有义务保证自己数据的信息安全等，提示个人注重信息保护等。

A.2.3 传输安全

宜采用校验技术或密码技术保证个人健康医学数据在传输过程中的保密性、完整性。加密方法的选择宜考虑应用场景、传输方式、数据规模、效率要求等，设备宜默认开启数据加密功能。

全国团体标准信息平台 中国标准出版社

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] T/CESA 1049—2018 区块链 隐私保护规范

[3] T/CESA 1109—2020 智能医疗影像辅助诊断系统技术要求和测试评价方法

[4] T/NAHIEM 47—2022 医学影像数据人工智能分析方法评估规范

[5] IEEE P3652.1 Guide for Architectural Framework and Application of Federated Machine Learning

[6] ISO/IEC 20889:2018 Privacy enhancing data de-identification terminology and classification of techniques

全国团体标准信息平台 中国标准出版社