



团 体 标 准

T/SCGS 313007—2024

隐私增强的医学影像联合建模规范

Privacy-enhanced joint modeling specifications for medical imaging

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

前言 III

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 3

5 医学影像数据联合建模流程与隐私增强 3

附录 A（规范性） 联合建模的性能指标 10

参考文献 12

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。

隐私增强的医学影像联合建模规范

1 范围

本文件规定了医学影像数据联合建模的流程与规范。

本文件适用于医学影像数据联合建模的各种流程,包括建模、评价、部署等范围。

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

医学影像 **medical imaging**

利用医学成像设备及技术所得到的图像。

3.2

数据隐私 **data privacy**

一个数据保护领域,涉及正确处理敏感数据,尤其是个人数据以及其他机密数据。

注:包括某些财务数据和知识产权数据,以满足监管要求以及保护数据的机密性和不变性。

[T/CESA 1049—2018,定义 3.3,有修改]

3.3

隐私增强 **privacy-enhanced**

保护敏感信息隐私或机密性的技术方法。

注:隐私增强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,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,定义 3.3,有修改]

3.4

联邦学习 **federated learning**

一种多个参与方在保证各自原始数据不出数据方定义的可信域前提下,以保护隐私数据的方式交互中间数据,从而协作完成某项人工智能和机器学习任务的模式。

3.5

多方安全计算 **secure multi-party computation**

基于多方数据协同完成计算目标的密码技术,获得除计算结果及其可推导出的信息之外,不会泄漏各方隐私数据。

注:多方安全计算常采用的技术有混淆电路、不经意传输、秘密分享、同态加密等。

3.6

差分隐私 **differential privacy**

一种数据共享手段,实现仅分享可以描述数据库的一些统计特征,而不公开具体个人信息的。