ICSxx.xxx.xx
CCS X xx

团 体 标 准

JH/CAA 008-2025

多模态专病数据平台总体技术要求

Overall Technical Specifications for a Multimodal Disease-Oriented Data Platform

（征求意见稿）

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

2026-XX-XX 发布 2026-XX-XX 实施

中国自动化学会 发布

目　　次

前　言

本文件按照GB/T1.1—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。

本文件由中国自动化学会提出并归口。

本文件起草单位：电子科技大学、四川大学华西医院、成都无限空间智能科技有限公司、天府锦城实验室。

本文件主要起草人：殷晋等。

多模态专病数据平台总体技术要求

1 范围

本文件规定了多模态专病数据平台的总体技术架构、功能要求、安全管理要求、运维要求以及互联互通要求。

本文件适用于面向特定专病，开展多源异构医疗数据采集、治理、融合、分析与共享的信息系统的设计、研发、部署与管理。相关医疗卫生机构、医药机构、研究机构及企业可参照使用。

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 25000.12-2017 系统与软件工程 系统与软件质量要求和评价 (SQuaRE) 第 12 部分：数据质量模型

GB/T 34960.5-2018 信息技术服务 治理 第 5 部分：数据治理规范

GB/T 35295-2017 信息技术 大数据 术语

GB/T 39725-2020 信息安全技术 健康医疗数据安全指南

WS/T 671-2020 国家卫生与人口信息数据字典

DICOM 标准（现行版） 医学数字成像与通信标准

GB/T 22239-2019 信息安全技术 网络安全等级保护 基本要求

GB/T 25070-2019 信息安全技术 网络安全等级保护 安全设计技术要求

GB/T 22240-2020 信息安全技术 网络安全等级保护 定级指南

GB/T 18336.2-2024 网络安全技术 信息技术安全评估准则 第 2 部分：安全功能组件

GB/T 18018-2019 信息安全技术 路由器安全技术要求

GB 50174-2017 数据中心设计规范

3 术语和定义

GB/T 35295-2017 和 GB/T 36344-2018 界定的以及下列术语和定义适用于本文件。

3.1

多模态数据 （Multi-Modal Data）

在医学研究与临床应用中，联合利用来自不同信息来源或表现形式的数据，对同一疾病或研究对象进行描述与分析的方式，常见模态包括医学影像、临床文本及结构化临床数据等。

3.2

专病 （Disease-Specific）

在数据访问与操作过程中，根据用户身份、角色和策略进行权限判定与控制的系统组件。

3.3

多模态专病数据平台（Multi-Modal Disease-Specific Data Platform）

面向特定专病（如肿瘤等），支持影像、文本、结构化数据等多源异构医疗数据的采集、治理、融合、分析与共享的信息系统。

3.4

数据主体 （Data Subject）

在本平台数据处理活动中，特指其个人健康数据被处理的自然人（即患者），依法享有知情、访问、更正、删除及撤回授权同意等权利。平台有义务提供清晰便捷的渠道，保障数据主体有效行使这些权利。

4 缩略语

下列符号和缩略语适用于本文件。
AI：人工智能 (Artificial Intelligence)
EMR：电子病历 (Electronic Medical Record)
PACS：影像存档与通信系统 (Picture Archiving and Communication System)
HL7：国际医疗信息交换标准 (Health Level Seven)
FHIR：快速医疗互操作性资源 (Fast Healthcare Interoperability Resources)
DICOM：医学数字成像与通信标准 (Digital Imaging and Communications in Medicine)
VPN：虚拟专用网络 (Virtual Private Network)
SSO：单点登录 (Single Sign-On)
API：应用程序编程接口 (Application Programming Interface)
TLS：传输层安全协议 (Transport Layer Security)

5 功能结构和处理流程

5.1 功能框架

多模态专病数据平台包括平台支撑层、数据应用层、运维管理与安全管理四个方面，其中平台支撑层是支撑平台运行与安全的核心技术与系统，包括多模态数据采集与集成、数据治理与标准化、数据集成与融合、核心权限引擎以及安全与隐私保护等，平台互联互通系统支持平台之间的互联互通与互操作，便于提供跨平台的集约化服务。数据应用层包括数据登记、数据流通、授权管理与数据运营

等功能系统，支持全流程的平台服务。多模态专病数据平台参考架构见图 1。

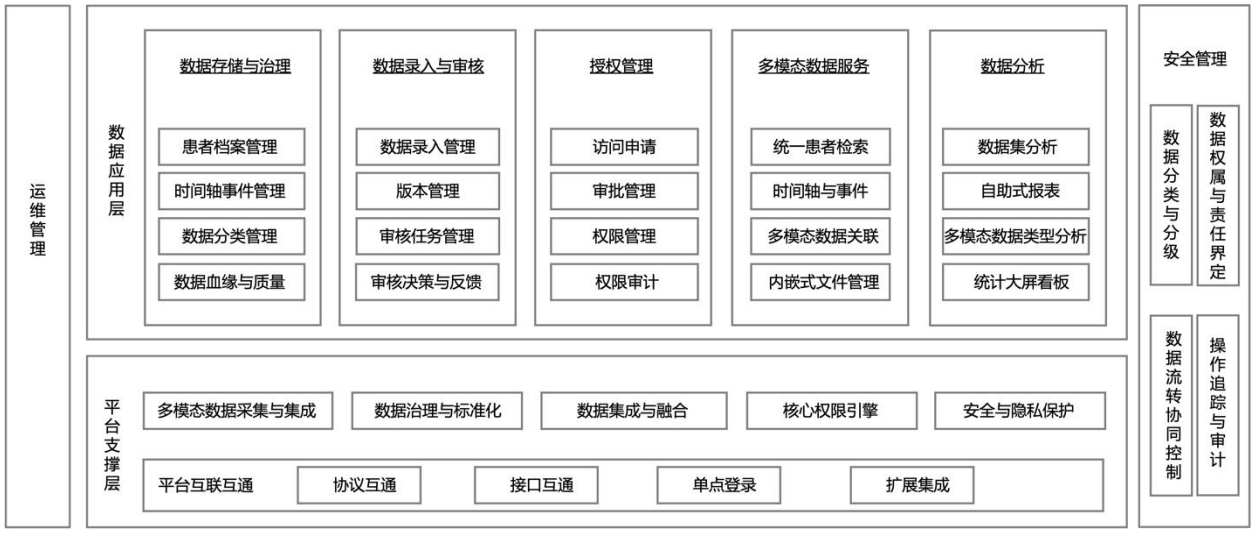

图 1 多模态专病数据平台功能框架

5.2 主要流程

多模态专病数据平台的操作流程见图 2。

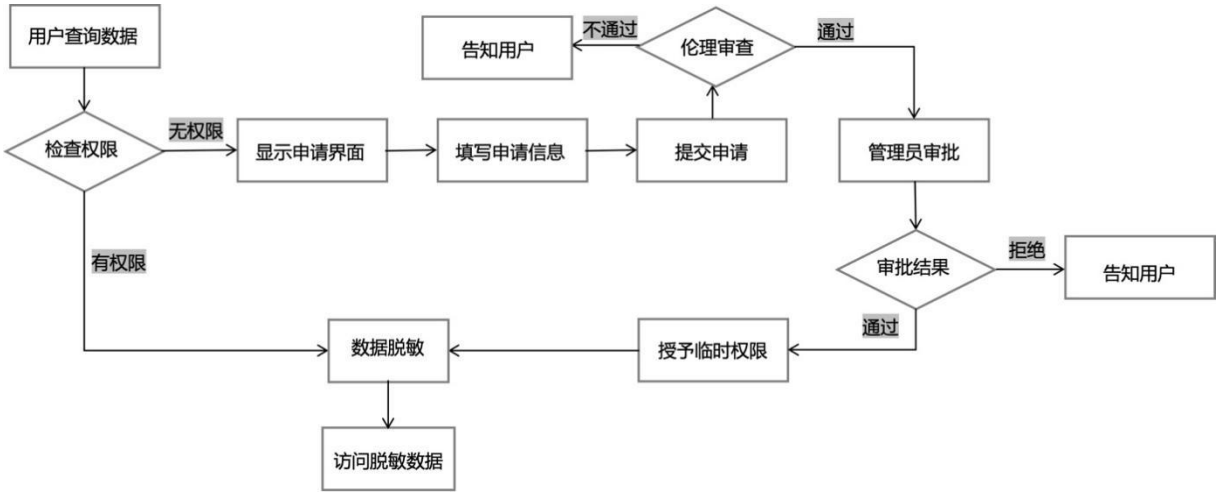

图 2 多模态专病数据平台流程

多模态专病数据平台应支持各方完成如下流程操作：

a) 用户查询数据：用户登录系统后，在数据平台中尝试查询或访问特定的数据资源。

b) 权限判断：系统接收到用户的数据查询请求后，自动检查该用户是否已经具备访问所请求数据的权限。

c) 有权限 → 进入数据访问准备流程：当系统验证用户已具备相应访问权限时，不直接返回原始数据，而是进入数据访问准备流程。

d) 无权限 → 显示权限申请入口：当系统判断用户不具备所需权限时，不直接显示数据内容，而应向用户展示权限申请入口及相关提示信息。

e) 填写申请信息：用户通过申请入口进入权限申请流程，按照要求填写数据使用目的、使用范围、使用期限等申请信息。

f) 提交申请：用户完成申请信息填写后，正式提交权限申请，系统生成唯一的申请编号，并将申请纳入审批流程。

g) 伦理审查：系统应支持对涉及医学专病数据的权限申请开展伦理审查。伦理审查未通过的，系统应终止后续流程并告知用户；伦理审查通过的，申请进入管理员审批环节。

h) 管理员审批：系统管理员或数据管理员对通过伦理审查的申请内容进行审核评估，并结合平台管理策略作出审批决策。

i) 审批决策判断：系统根据管理员审批结果进入相应分支流程。审批未通过的，应向用户反馈审批结果及相关说明。

j) 审批通过 → 授予权限：审批通过后，系统应按照申请内容为用户配置相应的数据访问权限，并限定访问范围和有效期限。

k) 数据脱敏处理：在数据实际提供或访问前，平台应对相关数据进行脱敏处理，确保个人敏感信息和隐私数据得到有效保护。

l) 访问脱敏数据：用户在获得授权后，仅可在平台规定的范围内访问经脱敏处理后的数据资源，并按照平台规则开展数据使用活动。

6 功能要求

6.1 数据存储与治理

6.1.1 患者档案管理

患者档案管理应符合以下要求：

a) 应支持基于身份证号或等效唯一标识进行全库查重；

b) 当发现重复记录时，应提示操作人员并提供合并选项，避免重复建档；

c) 对于新患者，应自动生成唯一的内部脱敏 ID，并建立主索引；

d) 统应保证患者档案数据的唯一性、准确性和可追溯性。

6.1.2 时间轴事件管理

时间轴事件管理应符合以下要求：

a) 应提供基于时间轴的患者全生命周期事件管理界面；

b) 应支持为患者添加、编辑或标注医疗事件（如初诊、手术、放疗周期、随访等）；

c) 每个事件应作为时间节点挂载，并支持与结构化表单数据和非结构化文件（如放疗剂量表、病理报告等）关联；

d) 应以时间为线索直观展示患者的全生命周期医疗数据。

6.1.3 数据血缘与质量管理

数据血缘与质量管理应符合以下要求：

a) 应记录数据来源、处理日志和访问痕迹，确保可追溯，其治理过程宜符合 GB/T 34960.5-2018 的相关要求；

b) 应对录入数据执行格式、完整性等基础质量校验，并在必要时提示异常，质量要求可参照 GB/T 25000.12-2017；

c) 应为数据审核、溯源和后续模型训练提供可靠依据。

6.2 数据录入与审核

6.2.1 数据录入管理

数据录入管理应符合以下要求：

d) 应提供结构化数据录入表单；
e) 应支持对表单字段配置验证规则，包括数值范围、必填项等；
f) 应保证录入数据仅在通过预定义规则校验后方可写入数据库。

6.2.2 版本管理

版本管理应符合以下要求：

a) 用户保存未完成数据时，应将其存储为“草稿”状态，仅创建者本人可见和可修改；
b) 草稿提交后应变为“待审核”版本；
c) 被审核驳回的数据应返回提交者，提交者修改后可再次提交；
d) 审核通过的数据应保存为正式版本，并锁定防止随意更改。

6.2.3 审核任务管理

审核任务管理应符合以下要求：

a) 当数据被提交后，应根据预设规则（如按数据分类或项目）自动分配审核任务；
b) 应支持通过站内信或邮件通知审核人员；
c) 应实现审核流程的自动化流转，提高审核处理效率。

6.2.4 审核决策与反馈

审核决策与反馈应符合以下要求：

a) 审核员界面应集中显示待审数据；
b) 审核员应能够查看数据详情并对比修改历史；
c) 审核员应能够对数据做出“通过”或“驳回”决策；
d) 审核驳回时，应要求审核员填写明确的理由；
e) 应根据审核决策自动更新数据状态，并通知提交者。

6.3 授权管理

6.3.1 访问申请

访问申请应符合以下要求：

a) 应支持用户查看其当前可访问的数据范围；
b) 对于无访问权限的数据，应提供申请入口；
c) 应引导用户填写申请内容，并要求填写详细的学术用途说明；
d) 应将申请单自动提交至审批流程。

6.3.2 伦理审查

伦理审查应符合以下要求：

a) 应支持针对涉及医学专病数据的访问申请开展伦理审查，并将伦理审查作为数据授权的前置条件；
b) 应支持对申请的研究目的、数据使用范围、使用期限及合规性进行审查；
c) 对未通过伦理审查的申请，应终止后续审批流程，并向用户反馈审查结果及原因；
d) 对通过伦理审查的申请，应自动流转至后续的管理员审批环节。

6.3.3 审批管理

审批管理应符合以下要求：

a) 应接收来自用户的访问申请；

b) 应根据数据敏感度、数量等因素，将申请自动路由至指定审批人（如项目负责人、伦理管理员）；

c) 应支持多级审批流程；

d) 审批人应能够查看申请详情，并执行“批准”、“拒绝”或“要求补充信息”的操作。

6.3.4 权限管理

权限管理应符合以下要求：

a) 应在申请获批后，根据策略授予有明确时间限制的临时访问权限（如 3 个月）；

b) 应包含定时任务机制，到期前提醒用户，并在到期后自动回收权限；

c) 应确保权限的动态管控与数据安全。

6.3.5 权限审计

权限审计应符合以下要求：

a) 应为管理员提供查询功能，可统计和查看任意用户当前拥有的所有权限；

b) 应记录并可追溯权限授予历史；

c) 应支持对用户数据访问行为进行记录和统计；

d) 统应满足内部审计与合规性检查的要求，确保权限授予的合理性和可追溯性。

6.4 多模态数据服务

6.4.1 统一患者检索

统一患者检索应符合以下要求：

a) 应提供全局搜索功能，支持基于患者脱敏 ID、诊断信息等关键词进行模糊查询；

b) 应通过权限控制引擎对检索结果进行过滤，仅返回用户有权访问的患者数据；

c) 应保证检索过程和结果的安全性与合规性。

6.4.2 时间轴与事件

时间轴与事件管理应符合以下要求：

a) 应在患者详情页中提供可视化时间轴，标记患者关键医疗事件；

b) 用户点击时间轴事件节点时，应能自动定位并展开对应的结构化记录与非结构化文件；

c) 应提供基于时间的直观导航，支持患者全生命周期数据的浏览与追溯。

6.4.3 多模态数据关联

多模态数据关联应符合以下要求：

a) 应支持在查看某次医疗事件时，自动关联展示该事件产生的多模态数据；

b) 应在界面中实现结构化数据与非结构化数据的并行展示，例如结构化“危及器官剂量表”与“剂量分布图”预览；

c) 应支持影像类数据的放大预览，确保数据可读性和交互便捷性。

6.4.4 内嵌式文件管理

内嵌式文件管理应符合以下要求：

a) 应支持非结构化文件（如 PDF 报告、影像截图）的在线预览，无需本地下载即可查看；

b) 应利用浏览器原生能力或集成轻量级预览组件，实现文件的安全可控访问；

c) 应避免文件的本地扩散，提升用户体验与数据安全性。

6.5 数据分析

6.5.1 数据集分析

数据集分析应符合以下要求：

a) 应支持用户根据多种条件（如数据集名称、数据来源、数据维度等）进行复合查询；

b) 应支持基于不同维度对数据集进行分析；

c) 应保证分析过程符合权限控制要求，确保数据合规。

6.5.2 自助式报表

自助式报表应符合以下要求：

a) 应支持用户从字段列表中选择分析变量（如年龄、TNM 分期、放疗剂量等）；

b) 应支持用户选择图表类型（如柱状图、散点图等），并自动生成统计图表；

c) 应在后台对所有查询执行权限控制，确保数据安全；

d) 应支持报表的可视化展示与交互操作。

6.5.3 多模态数据类型分析

多模态数据类型分析应符合以下要求：

a) 应支持对集成的多源异构医疗数据进行统计分析；

b) 应保证不同模态数据的分析结果能够统一展示和比较；

c) 应支持跨模态数据的联合统计和结果导出。

6.5.4 统计大屏看板

统计大屏看板应符合以下要求：

a) 应支持面向管理与决策层的可视化展示；

b) 应动态展示平台核心指标，提供多维度统计图表（如患者分布、解剖位置分布等）；

c) 应支持实时刷新与交互功能，提供宏观的业务洞察；

d) 应具备扩展能力，以满足不同业务场景的定制化需求。

6.6 多模态数据处理

多模态数据处理是平台支撑层的重要组成部分，为上层应用提供统一、可靠的数据支撑。处理后的高质量数据可用于临床决策支持、科研分析及人工智能（AI）模型训练等场景。多模态数据处理包括：多模态数据采集与集成、数据治理与优化、数据集成与融合、核心权限引擎、安全与隐私保护。

6.6.1 多模态数据集采集与集成

多模态数据集采集与集成应符合以下要求：

a) 应支持多模态医疗数据的采集，涵盖从电子病历 (EMR)、实验室信息系统中获取的结构化数据，从临床文档中获取的非结构化文本数据，以及从影像存档与通信系统 (PACS) 等系统中获取的医学影像数据；

b) 应支持多源数据的接入与标准化处理，实现跨机构、跨平台的数据集成；

c) 应确保采集与集成过程的数据完整性和一致性。

6.6.2 数据治理与优化

数据治理与优化应符合以下要求：

a) 应支持数据清洗、标准化和格式校验，提升数据质量；

b) 应具备元数据管理能力，支持数据溯源与分类管理；
c) 应提供数据质量监控与优化机制，确保数据的准确性与可用性。

6.6.3 数据集成与融合

数据集成与融合应符合以下要求：
a) 应支持跨模态、跨系统的数据对齐与语义映射；
b) 应支持多源数据的特征融合，保证语义一致性；
c) 应确保融合后的数据可用于上层应用的联合分析与建模。

6.6.4 核心权限引擎

核心权限引擎应符合以下要求：
a) 应内置权限控制机制，支持基于角色、属性和策略的访问控制；
b) 应确保用户仅能在授权范围内访问、处理和分析数据；
c) 应具备细粒度的权限配置和动态调整能力。

6.6.5 数据脱敏处理

数据脱敏处理应符合以下要求：
a) 平台应在数据被访问或使用前，对涉及个人敏感信息的医学专病数据进行脱敏处理，相关安全要求应符合 GB/T 39725-2020；
b) 数据脱敏应由平台侧统一实施，并根据数据类型和使用场景采用相应的脱敏策略；
c) 脱敏处理后，数据应在不影响数据可用性的前提下，降低对个人身份和隐私信息的识别风险；
d) 平台应确保用户仅可访问脱敏处理后的数据资源，并按照授权范围和使用目的使用相关数据。

6.6.6 安全与隐私保护

安全与隐私保护应符合以下要求：
a) 应支持数据脱敏与加密存储，保障敏感信息安全；
b) 应记录访问与操作日志，实现可追溯性和合规审计；
c) 应满足国家及行业相关安全与隐私保护规范要求。

7 安全管理要求

7.1 数据分类与分级

本节根据国家相关标准，规定了健康医疗数据的分类体系与安全分级要求。平台必须依据本节对所有数据进行分类与分级，并以此作为实施差异化安全防护与访问控制策略的基础。

7.1.1 数据类别范围

平台处理的数据依据其内涵和属性，应划分为以下类别。分类原则参照 GB/T 39725-2020 与 WS/T 671-2020：
a) 个人属性数据：能够单独或与其他信息结合识别特定自然人的数据。包括但不限于：
   1) 人口统计信息：姓名、出生日期、性别、民族、国籍、职业、住址等。
   2) 个人身份信息：身份证号、工作证、社保卡、影像画像、健康卡号等。
   3) 个人通讯信息：电话号码、邮箱、账号及关联信息等。
   4) 个人生物识别信息：基因、指纹、声纹、虹膜、面部特征等。
b) 健康状况数据：反映个人健康情况或与之有密切关系的数据。包括但不限于主诉、现病史、

既往病史、家族史、体格检查、遗传咨询、生活方式、基因测序、蛋白质分析等。

c) 医疗应用数据：反映医疗服务情况的数据。包括但不限于病历、医嘱、检验检查报告、用药记录、手术记录、护理记录、知情同意书等。

d) 医疗支付数据：医疗或保险服务中涉及的与费用相关的个人数据。包括医疗交易信息和保险信息等。

e) 卫生资源数据：反映卫生服务人员、卫生计划和卫生体系能力与特征的数据。

f) 公共卫生数据：关系到国家或地区大众健康的专业相关数据。

7.1.2 数据安全流程与分级

平台应依据数据的重要程度、风险等级以及可能造成的损害，将数据划分为 5 个安全级别。整体步骤如图 3 所示，包括：

a) 业务申请：数据防护需求由相关业务部门提出。

b) 安全级别审核：根据敏感度和业务重要性，确定数据的安全级别与类型。

c) 上报保护系统匹配规则：填写数据防护申请表，提交系统进行规则匹配。

d) 分级判定：依据分类算法及安全等级标准，确定最终安全等级。

e) 策略生成与下发：生成相应的数据防护策略并下发实施。

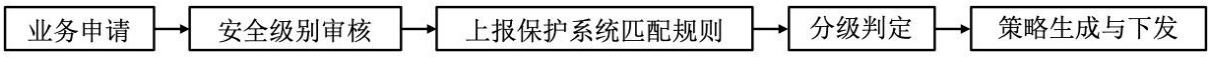

图 3 数据分类分级防护流程

根据数据重要程度、风险等级以及对个人或机构可能造成的影响，平台应将数据划分为以下五级，其分级保护要求应不低于 GB/T 22240-2020 与 GB/T 22239-2019 中对应级别的规定：

a) 第 1 级：公开数据

定义：可完全公开使用的数据。

控制要求：可直接在互联网面向公众公开。在存储和传输中可不进行加密处理。

b) 第 2 级：内部共享数据

定义：可在较大范围内访问使用的数据，经处理后不能标识个人身份。

控制要求：数据在共享前应经过完全脱敏处理，确保不可识别个人身份。内部用户需经安全认证和流程审批后，通过访问控制策略获取数据访问权限。

c) 第 3 级：受控访问数据

定义：在中等范围内访问使用的数据，如未经授权披露，可能对个人造成中等程度的损害。该类数据经过部分去标识化处理，但仍可能重标识。

控制要求：数据在存储时应采用部分加密或数据屏蔽技术（例如对姓名、身份证等关键字段加密）。访问权限仅限于授权项目组，需严格执行安全认证和访问控制策略。可考虑使用数据水印技术，以便于追踪潜在的数据泄露。

d) 第 4 级：限制访问数据

定义：在较小范围内访问使用的数据，如未经授权披露，可能对个人造成较高程度的损害。该类数据可直接标识个人身份。

控制要求：数据在存储和传输中应采用完全加密措施。应实施基于角色的、精细化的访问控制和严格的安全认证（如多因素认证）。所有访问行为必须被深度审计。

e) 第 5 级：严格限制访问数据

定义：仅在极小范围内且在严格限制条件下供访问使用的数据，如未经授权披露，会对个人造成严重程度的损害。

控制要求：应采用最高级别的安全防护。在第 4 级控制要求的基础上，进一步收紧访问权限，仅授权

给极少数核心人员。所有访问申请应该经过多级审批流程，且应能根据申请动态生成并下发临时性的、最小化的防护策略，安全设计技术要求可参照 GB/T 25070-2019。

7.2 数据权属与责任界定

7.2.1 数据主体权利

数据主体（即患者）是其个人健康信息的最终所有者，依法享有对其数据的知情权、访问权、更正权、删除权以及撤回授权同意权。平台应提供清晰、便捷的渠道，以保障数据主体能够有效行使其法定权利。

7.2.2 数据提供方权责

数据提供方（如各医疗中心）是其所采集和提供数据的控制者。数据提供方权责要求如下：

a) 应确保数据采集的合法合规性，并已获得数据主体的有效授权同意。
b) 对所提供数据的原始真实性、准确性和完整性负责。
c) 应按照第四章 数据标准化的要求对数据进行预处理和标准化。
d) 在数据上传至平台前，应完成必要的本地化脱敏处理。
e) 有权了解其所提供数据在平台内的使用情况，并对超出授权范围的使用行为提出异议。

7.2.3 平台运营方权责

平台运营方是平台基础设施和数据处理活动的管理者。平台运营方要求如下：

a) 应负责平台的建设、运维和安全保障，确保平台的稳定、可靠、安全运行。
b) 为各方提供技术支持，监督数据共享协议的执行情况。
c) 不得将平台数据用于数据共享协议约定之外的任何目的。
d) 在发生数据安全事件时，应立即启动应急预案并向相关方通报。
e) 应建立并严格执行访问控制、安全审计、数据加密等安全策略。

7.2.4 数据使用方权责

数据使用方（如科研人员）是经授权的数据处理者。数据使用方要求如下：

a) 应经伦理审查和审批后方可使用。
b) 应严格遵守数据共享协议和研究方案，仅在授权范围内使用数据。
c) 严禁尝试对数据进行再识别或关联分析以获取数据主体身份。
d) 应承担对从平台获取的数据（如有）保管责任，不得擅自传播、复制或转让。
e) 研究结束后，应按规定销毁本地持有的数据副本。

7.2.5 数据共享协议

数据共享协议要求如下：

a) 所有参与方在使用平台前，应共同签署具有法律约束力的数据共享协议。
b) 协议应明确规定数据的使用目的、共享范围、各方权责、保密义务、数据安全要求、知识产权归属以及违约责任等核心条款。

7.3 数据流转协同控制

所有数据流转活动应在预定义的策略和协议框架下进行，旨在实现“数据可用不可见、使用可控可计量”的目标，最大限度降低数据在共享过程中的泄露风险。

7.3.1 安全共享协议与接口规范

在多模态专病数据平台中，安全共享协议与接口规范是保障数据跨系统交互、跨机构共享和合规使用的关键环节。其设计不仅关系到数据传输的可靠性与保密性，也直接影响到平台的安全性、可追

溯性和合规性，其要求如下：

a) 接口安全：

1) 平台应通过安全的应用程序编程接口（API）提供数据服务，所有 API 应基于 HTTPS 协议（强制使用 TLS 1.3 或更高版本）进行通信，确保传输安全符合 GB/T 39725-2020 的相关规定。

2) 应采用基于 OAuth 2.0 或同等安全强度的框架对 API 调用进行认证和授权。

3) 所有 API 接口的访问权限应与 6.4.2 中定义的角色访问控制策略严格绑定，确保用户只能调用其角色权限范围内的接口。

b) 数据交换格式：

1) 结构化和半结构化数据的交换应采用标准化的数据格式（如 JSON），并提供清晰、统一的格式定义。

2) 对于医学影像等非结构化数据，应遵循 DICOM 等行业标准进行接口交互。

c) 接口访问控制：

1) 应对来自外部的 API 请求实施严格的来源 IP 地址白名单控制，网络边界安全要求可参照 GB/T 18018-2019。

2) 应部署 API 网关，对所有请求进行流量控制、速率限制和恶意请求过滤，以防范拒绝服务（DoS）攻击和 API 滥用。

d) 接口日志与审计：

1) 应对每一次 API 调用进行完整的日志记录，日志内容应包括请求来源、用户身份、调用的接口、请求时间、请求参数和返回结果。

2) API 日志应作为安全审计的重要依据，并按规定进行存储和保护。

7.3.2 跨机构数据传输加密

跨机构数据传输是最常见且最敏感的环节之一。若传输过程缺乏安全保护，可能导致患者隐私泄露、数据篡改或非法拦截。为确保跨机构数据交换的机密性、完整性和合规性，平台必须采用严格的加密。加密要求如下：

a) 传输链路加密：

1) 重申所有跨越机构边界的数据传输，必须在加密信道中进行。加密协议及强度应符合 GB/T 39725-2020 及 GB/T 18336.2-2024 的相关要求。

2) 对于机构与平台之间的服务端到服务端数据同步或交换，应采用双向 TLS 认证，即通信双方必须互相验证对方的数字证书，以确保端点的合法性。

b) 数字证书管理：

1) 用于传输加密和身份认证的数字证书应由受信任的证书颁发机构签发。

2) 应建立证书生命周期管理制度，确保证书在有效期内使用，并及时进行续期或吊销。

c) 虚拟专用网络：于需要进行批量数据传输或建立持续连接的场景，应在参与机构和中心平台之间建立基于 IPsec 协议的站点到站点 VPN 隧道，以提供网络层级的隔离和保护。隧道安全应符合 GB/T 18018-2019 的相关要求。

d) 数据完整性校验：在数据传输过程中，应采用校验和（如 SHA-256）或数字签名等机制，确保接收方验证数据在传输过程中未被篡改。

7.3.3 联邦学习等隐私计算平台技术

本节为增强性要求，适用于具备分布式协作建模能力的高安全等级平台。

a) 应采用同态加密或安全多方计算技术实现梯度聚合；

b) 应对上传参数应用差分隐私机制并论证隐私预算；

c) 若采用可信执行环境，应提供远程证明机制。

7.4 操作追踪与审计

7.4.1 日志记录内容与保护

7.4.1.1 日志覆盖范围

记录日志覆盖范围要求如下：

a) 用户活动日志：包括但不限于用户登录（成功与失败）、注销、密码修改、权限变更申请与审批。

b) 数据访问日志：对所有数据的核心操作，包括查看、查询、上传、下载、修改、删除等。

c) 系统运行日志：平台应用和系统组件的启动、停止、关键配置变更、系统错误和异常。

d) 安全事件日志：由安全设备或策略生成的告警，如防火墙拦截、入侵检测告警、API 异常调用等。

7.4.1.2 日志格式与保护

日志格式与保护要求如下：

a) 日志应采用结构化的格式（如 JSON）进行记录，以便于机器解析和自动分析。

b) 日志记录应具备防篡改能力。应将日志实时或准实时地发送至独立、安全的中央日志管理系统中进行统一存储。

c) 日志的访问权限应严格受控，仅允许审计员和授权的系统管理员访问。

d) 所有日志的在线存储时间不应少于 6 个月，并应根据法规要求进行离线归档。

7.4.2 操作行为溯源与审计机制

平台的操作安全管理应覆盖认证、账户、授权、审计、登录记录与操作记录等环节，环节要求如下：

a) 唯一认证：所有访问均需经过统一身份认证，不得使用共享账号；

b) 账户管理：账户分配、启用与注销必须遵循最小权限原则；

c) 授权管理：所有权限授予需基于审批，做到可追溯；

d) 审计机制：所有访问操作必须记录，并接受周期性检查；

e) 记录留存：平台必须保留详细的登录记录和操作日志，确保事后可追溯。

7.4.2.1 审计周期与范围

审计周期与范围要求如下：

a) 平台运营方应指定独立的审计员角色，定期（至少每季度一次）对日志进行审查。

b) 审计的重点应包括：特权账户的操作行为、所有失败的登录尝试、高频或批量数据访问行为、所有数据下载记录以及权限变更操作。

7.4.2.2 审计技术支持

审计技术支持要求如下：

a) 应部署安全信息和事件管理或类似系统，对海量日志进行自动化关联分析，并配置告警规则以实时发现可疑行为模式。

b) 审计应提供强大的检索和溯源功能，能够实现：

1) 根据用户 ID，追溯其在特定时间段内的所有操作。

2) 根据数据 ID，追溯其被所有用户访问和操作的全过程历史。

7.4.2.3 审计报告

审计报告要求如下：

a) 每次定期审计都应形成正式的书面审计报告。

b) 报告应记录审计的范围、过程、发现的问题、潜在风险，并提出整改建议。审计报告应存档备查。

7.4.3 数据加密与存储安全要求

7.4.3.1 静态数据加密

静态数据加密要求如下：

a) 平台中存储的所有敏感数据，包括数据库文件、影像文件、文本报告、日志和备份数据，应采用符合国家密码管理要求的加密算法（如国密算法 SM1、SM2、SM3、SM4 等）进行加密存储。核心存储设施的安全物理环境应满足 GB 50174-2017 中关于数据中心安全的规定。

b) 加密密钥与加密数据应分离存储和管理。

7.4.3.2 传输数据加密

传输数据加密要求如下：

a) 平台内外所有的数据传输，包括用户访问、跨中心数据汇聚等，应使用安全的加密传输协议（如 TLS 1.3 或更高版本，或国密 SSL 协议）。

b) 应禁用所有不安全的、明文传输的协议。

7.4.3.3 密钥管理

秘钥管理要求如下：

a) 应建立一套覆盖密钥生成、分发、存储、使用、轮换、归档和销毁全生命周期的安全管理机制。

b) 应使用经认证的密钥管理系统或硬件安全模块来保护根密钥和关键加密密钥。

c) 密钥的访问权限应遵循最小权限原则，并记录所有对密钥的访问和操作。密钥管理系统的安全评估可参考 GB/T 18336.2-2024。

8 运维要求

多模态专病数据平台应符合 GB/T 28827.1-2022 与 GB/ T 28827.6-2019 的相关要求。

9 互联互通要求

9.1 协议互联

支持基于数字对象架构的数联网等协议化方式，实现平台之间的配置式组网互联。应支持跨平台的数据传输和信息交换，确保系统间的互操作性和互联互通，从而提升整体互联效率与能力。

9.2 接口互通

多模态专病数据平台应支持接口互通，便于支持平台之间的规模化服务。接口互通应符合以下要求：

a) 对外应提供基于 RESTful 等方式的标准化接口，接口设计宜遵循 HL7 FHIR 等医疗健康信息交换标准，至少应支持申请审核、目录查询、业务集成、权限同步等功能；

b) 应定义统一的接口规范与接口文档，内容应包括接口地址、请求方法、请求参数、返回格式等，以确保不同系统之间接口调用的兼容性和一致性。

9.3 单点登录

应提供单点登录（SSO）功能，确保用户可通过一次登录认证，在跨平台环境中按权限访问所需资源，提升用户体验并简化跨平台身份管理。

9.4 扩展集成

9.4.1 二次授权集成

多模态数据平台应支持面向二次授权场景的扩展集成功能。平台应通过提供二次授权业务接口，允许数据需求方在其业务系统中嵌入该接口。当触发二次授权条件时，相关个人应能够通过该接口提供明确的二次授权信息。平台应将该二次授权信息与操作日志一并记录，并支持基于区块链或等效技术进行存证，以确保授权过程的可追溯性与合规性。

9.4.2 其他系统集成

多模态数据平台应支持与外部关键系统的集成，包括但不限于：区域法人库、统一身份认证平台、实名制认证平台以及科研伦理审查系统。平台应能够从这些系统中获取并验证相关信息，以实现身份认证、合规验证和跨机构协同的数据服务，保障数据流通的安全性与合规性。

资料性附录 A

A.1 乳腺癌新辅助放疗联合免疫治疗示例

附录该节给出了多模态专病数据平台在乳腺癌新辅助治疗研究场景中的应用示例，用于说明本文件所规定的总体技术架构和功能要求在实际医学研究中的应用方式。

四川大学华西医院围绕乳腺癌新辅助治疗相关研究需求，开展放疗联合免疫治疗在介入时机、剂量参数及分割方式等方面的探索性研究。研究过程中，结合临床数据、基础研究数据及大数据平台资源，构建多学科协同的数据支撑环境，用于支持乳腺癌新辅助治疗相关问题的系统分析。

在该研究场景中，通过对接医院 EMR、PACS 等系统，整合乳腺癌患者的多模态医学数据，探索与放疗联合免疫治疗相关的疗效预测因素、毒性相关因素及治疗反应差异等内容，并基于医学多模态数据库构建相应的数据分析与辅助决策支持机制。相关系统通过对多源异构数据的关联与处理，为乳腺癌放疗联合免疫治疗的研究与临床应用提供数据支持与参考依据。上述应用场景示例如图 4 和图 5 所示。

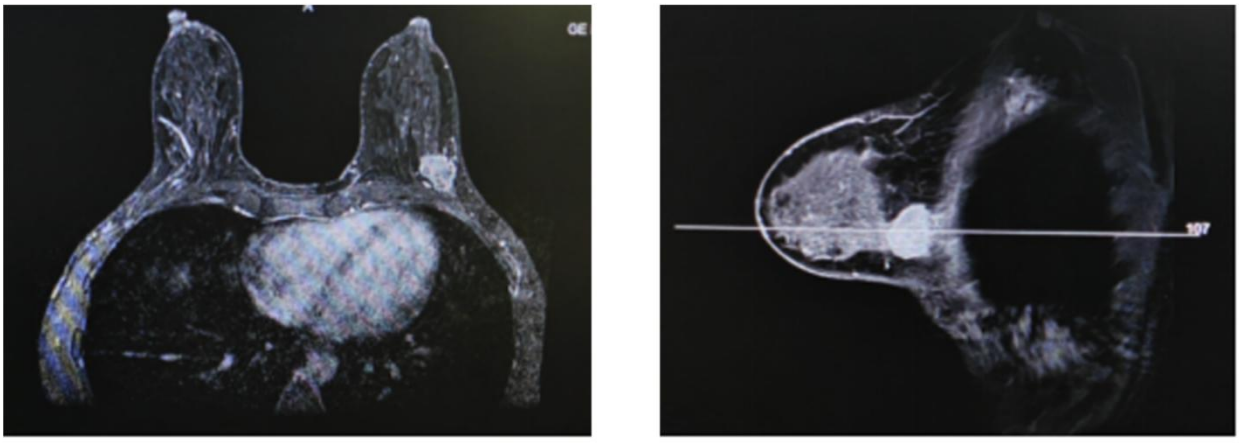

图 4 临床病例

Case	Pathological Type	Stage	Molecular Subtypes	Age	Subjects	Access	Updated
001	invasive carcinoma	cT2N0M0	TNBC	47	1	Preview	2025-04-24
002	invasive carcinoma	cT2N0M0	TNBC	37	1	Preview	2025-04-24
003	invasive carcinoma	cT2N0M0	TNBC	52	1	Preview	2025-04-24
004	invasive carcinoma	cT2N0M0	TNBC	32	1	Preview	2025-04-24
005	invasive carcinoma	cT2N0M0	TNBC	56	1	Preview	2025-04-24
006	invasive carcinoma	cT2N0M0	TNBC	30	1	Preview	2025-04-24
007	invasive carcinoma	cT2N0M0	TNBC	38	1	Preview	2025-04-24
008	invasive carcinoma	cT2N0M0	TNBC	47	1	Preview	2025-04-24
009	invasive carcinoma	cT2N0M0	TNBC	38	1	Preview	2025-04-24
010	invasive carcinoma	cT2N0M0	TNBC	36	1	Preview	2025-04-24

图 5 数据库样例

A.2 乳腺癌放疗免疫多模态数据平台构建示例

乳腺癌放疗免疫多模态数据平台构建示例如图 6 所示。

图 6 乳腺癌放疗免疫多模态数据平台门户

参考文献

[1] 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
[2] T/CECC 024-2023 公共数据授权运营平台技术要求
[3] DB54/T 0419-2024 大数据平台 总体框架参考