

团 体 标 准

T/ISC 0152—2026

医疗健康行业智能体 乳腺癌辅助诊疗技术 要求

Technical requirements for breast cancer diagnosis and treatment assistant intelligent agent
in the healthcare industry

（发布稿）

2026 - 09 - 08 发布

2026 - 10 - 08 实施

中 国 互 联 网 协 会 发 布

目 次

前 言 III

1 范围 4

2 规范性引用文件 4

3 术语和定义 4

4 缩略语 4

5 总体要求 4

6 必备功能要求 5

 6.1 患者数据整合 5

 6.2 临床工作智能辅助 5

 6.3 精准分期分型 5

 6.4 影像数据分析 6

 6.5 病理图像分析 6

 6.6 治疗方案推荐 6

 6.7 用药管理 7

 6.8 MDT 多学科会诊支持 7

 6.9 预后分析 8

 6.10 组学数据分析 8

 6.11 诊后随访 8

7 准确性要求 8

 7.1 模型验证规范 9

 7.2 模型比较与统计检验 9

 7.3 二分类任务 9

 7.4 文书生成类任务 9

 7.5 多分类任务 10

 7.6 图像类任务 11

8 智能体能力要求 11

 8.1 感知能力 11

 8.2 规划能力 12

 8.3 记忆能力 13

 8.4 执行能力 13

9 易用性要求 13

 9.1 可理解性 13

 9.2 易学性 14

 9.3 易操作性 14

10 安全性要求 14

 10.1 基础设施安全 14

 10.2 数据安全 15

10.3 应用安全	15
-----------------	----

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。

本文件由中国互联网协会归口。

本文件起草单位：北京协和医院、浙江省肿瘤医院、中国信息通信研究院、中国科学技术大学附属第一医院、中山大学孙逸仙纪念医院深汕中心医院、江苏省人民医院、中山大学附属第一医院、北京大学肿瘤医院、复旦大学附属肿瘤医院、四川省肿瘤医院、西安交通大学第一附属医院、上海市第十人民医院、上海交通大学附属第一人民医院、浙江大学医学院附属第一医院、天津市肿瘤医院、河北医科大学第四医院、复旦大学附属肿瘤医院、青岛大学附属医院、沐心数智医疗科技(北京)有限公司

本文件主要起草人：梁智勇、胡海、杜雨暄、贾斐、任九选、刘泊宁、张卓然、相识、陈冠衣、黄涂半特、潘跃银、陈凯、刘晓安、张赟建、范照青、胡欣、王浩、杨谨、盛媛、崔岱、顾鸣宇、张哲、郭晓静、刘月平、杨文涛、王成勤、凌连芷、齐立薇

本文件及其所代替文件的历次版本发布情况为：

医疗健康行业智能体 乳腺癌辅助诊疗

1 范围

本文件规定了医疗健康行业智能体 在乳腺癌辅助诊疗应用过程中涉及的技术能力，从功能要求、智能体能力要求、易用性要求和安全性要求等维度对智能体技术在乳腺癌辅助诊疗场景中应用的能力提出要求。

本文件适用于医疗健康行业智能体技术方开发乳腺癌辅助诊疗智能体时进行系统建设和应用范式参考，以及医疗机构等应用方参照进行乳腺癌辅助诊疗智能体选型。

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 35273-2020 信息安全技术 个人信息安全规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

医疗健康行业智能体 **healthcare ai agent**

在通用智能体的基础上，结合医疗健康行业特点设计的智能体，与医疗健康相关任务的适配度较高。

4 缩略语

下列缩略语适用于本文件

HIS: 医院信息系统 (Hospital Information System)

LIS: 实验室信息系统 (Laboratory Information System)

PACS: 影像归档与通信系统 (Picture Archiving and Communication System)

ER: 雌激素受体 (Estrogen Receptor)

PR: 孕激素受体 (Progesterone Receptor)

BI-RADS: 乳腺影像报告与数据系统 (Breast Imaging Reporting and Data System)

TNM: 肿瘤-淋巴结-转移分期系统 (Tumor/Node/Metastasis Staging System)

FISH: 荧光原位杂交 (Fluorescence In Situ Hybridization)

MRI: 磁共振成像 (Magnetic Resonance Imaging)

CT: 计算机断层扫描 (Computed Tomography)

5 总体要求

本文件规定了医疗健康行业智能体 乳腺癌辅助诊疗，包括功能完备性技术要求、准确性要求、智能体能力要求、易用性要求和安全性要求，该智能体仅用于辅助临床决策，不替代医师独立判断，不得在无医师确认情况下自动生成、变更或执行医嘱、处方及治疗方案，主要分为以下内容：功能完备性技术要求部分包括患者数据整合、精准分期分型、治疗方案推荐、组学数据分析、影像数据分析、预后分析、诊后随访、药物查询、MDT多学科会诊辅助、临床工作智能辅助；准确性要求部分包括二分类、多分类、文书生成及图像分割四项任务；智能体能力要求部分包括感知能力、规划能力、记忆能力和执行能力；易用性要求部分包括可理解性、易学性和易操作性；安全性要求部分包括基础设施安全、数据安全、应用安全。医疗健康行业智能体 乳腺癌辅助诊疗的架构图如图1所示。

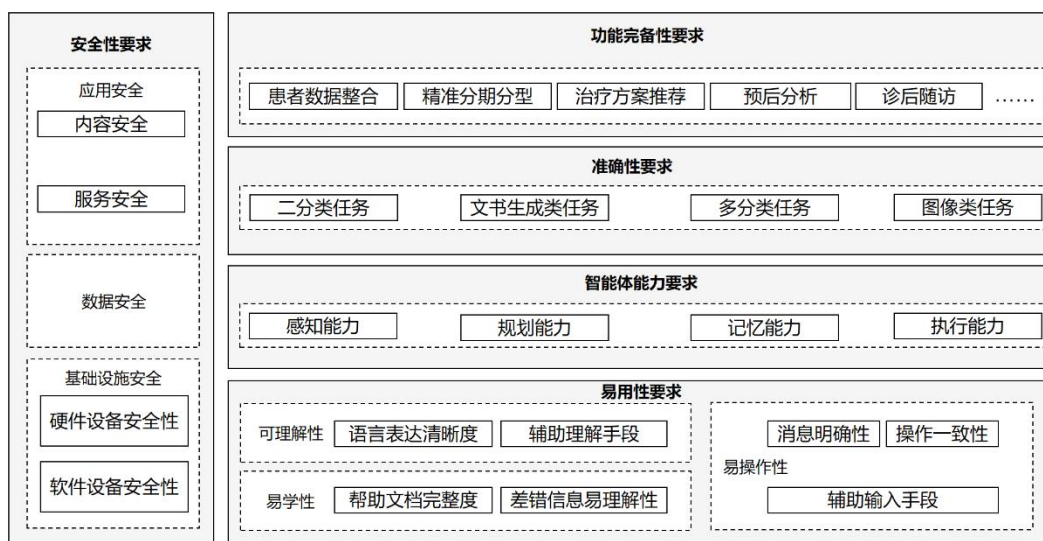


图 1 乳腺癌辅助诊疗智能体的架构示意图

6 必备功能要求

6.1 患者数据整合

乳腺癌辅助诊疗智能体应支持多源患者数据整合：

- 多模态数据接入：应支持集成来自院内信息系统（如 HIS、LIS、PACS 等）、可穿戴设备、患者上报及科研数据库的结构化与非结构化数据，包括但不限于：电子病历、乳腺 X 线摄影/超声/MRI 等影像原片及结构化报告、病理全切片图像、病理诊断报告、ER/PR/HER2/Ki-67 等关键免疫组化结果、BRCA1/2 等基因检测报告、CA15-3 等肿瘤标志物检验结果及随访记录；
- 数据融合与结构化：应支持利用自然语言处理、图像识别等技术，从病理图像、影像、分子测序、临床病历等数据源中自动提取乳腺病灶的 BI-RADS 分类、病理组织学相关字段（包括但不限于病灶位置、大小、转移情况、诊断名称、组织学类型、侵犯范围、切缘状态、淋巴结转移情况等）、TNM 分期描述、分子分型判定依据等关键医学实体与特征，并进行标准化、归一化处理，构建统一、时序性的患者数据；
- 质量校验与补全：应支持对接入数据的完整性、一致性进行自动校验，识别并预警关键信息的潜在矛盾与缺失，例如影像 BI-RADS 分类与病理结果不匹配、HER2(2+)但缺少 FISH 检测结果、缺失染色或切缘状态报告、图像缺失、图像与影像报告不一致等；内分泌与代谢相关数据字段的完整性校验应包括绝经状态判定所需信息（年龄、末次月经、卵巢手术史、化疗史）、性激素水平（FSH/E2）、甲状腺功能、空腹血糖/HbA1c、血脂及 DXA 骨密度结果；应支持基于医学知识图谱或算法模型提示补全建议并标记局限并给出提示，不应强行输出分析结果或诊断意见；
- 文书草稿自动生成：应支持基于整合后的数据一键生成入院记录、病程记录、出院小结、术前讨论小结等常用文书初稿，按医疗文书规范填入对应章节，供医生审核修改。

6.2 临床工作智能辅助

乳腺癌辅助诊疗智能体应支持对医生日常工作的辅助：

- 智能医学问答：应支持医生以自然语言方式提出诊疗相关的开放式问题，并基于方案知识库及外部知识库，生成带证据等级标注与来源引用的回答；
- 临床文书辅助生成：应支持基于整合的患者时序数据，一键生成入院记录、病程记录、出院小结、术前讨论小结等常用医疗文书的初稿，并自动填入分析结论，供医生审核修改后归档。

6.3 精准分期分型

乳腺癌辅助诊疗智能体应支持基于多维度数据的精准分期与分子分型：

- a) 多指南智能对照：应支持内置 TNM 等主流分期标准，并根据病理、影像、临床检查结果，明确标注所依据的指南名称及其发布年份，自动计算并推荐分期，同时对比展示不同版本指南或共识下的分期差异及诊断标准（基本诊断标准 vs. 理想诊断标准），并对临界值状态给出分层的临床解读；
- b) 分子分型智能判别：应支持结合 ER/PR、HER2、Ki-67 增殖指数等免疫组化及多组学检测结果，自动判定并报告 Luminal A、Luminal B、HER2 过表达型、TNBC 等分子亚型，并提示各生物标志物的临床意义及其对治疗方案选择的指导价值。应支持识别 HER2 低表达（HER2-low，即 IHC 1+或 2+且 FISH 阴性）的能力，将其作为独立的治疗类别进行标注，并关联相关靶向药物（如抗体药物偶联物 T-DXd 等）的治疗敏感性信息；
- c) 动态更新与回溯：当患者出现新发转移或复发时，应支持根据最新数据重新评估分期分型，并保留历史判定记录，支持病情演变的追踪分析；
- d) 临床模型可解释性：应支持基于 SHAP（Shapley Additive Explanations）方法的全局与局部特征重要性评估，明确各模态信息对分期分型与相关预测结果的贡献大小与方向；
- e) 绝经状态综合判定：应支持基于患者年龄、化疗史、卵巢手术史及 FSH/E2 等激素水平等数据，综合判定患者的绝经状态（绝经前、绝经后或围绝经期），并明确标注判定所依据的标准（如 STEEP criteria 等）及其不确定性，为内分泌治疗方案选择提供参考；
- f) 局限性提醒：应支持对低质量数据仅给出局限性提醒，不应输出意见。

6.4 影像数据分析

乳腺癌辅助诊疗智能体应支持专业的医学影像分析：

- a) 智能病灶识别与测量：应支持基于深度学习模型，对乳腺 X 线、超声、MRI 及 CT 影像数据中的病灶进行自动检测、分割、测量（如大小、形状、强化特征），并生成结构化报告；
- b) 模型决策可视化：应支持影像热图生成功能，将模型关注的关键区域以热图形式可视化呈现，辅助医生理解模型决策依据，并支持与已知病理学知识的一致性验证；
- c) 特征提取与预后关联：应支持提取影像组学特征，并与临床结局、分子分型等进行关联分析，挖掘深层次的影像生物学标志物。

6.5 病理图像分析

乳腺癌辅助诊疗智能体应支持对病理图像的智能化分析：

- a) 智能区域识别与分割：应支持基于深度学习模型，对 H&E 染色全切片图像中的乳腺肿瘤区域、浸润性癌灶、导管内原位癌（DCIS）区域、淋巴结转移灶等进行自动检测、边界分割与面积量化，辅助病理医师快速定位关键区域；
- b) 组织学分级与分型判定：应支持依据 Nottingham 分级系统自动提取腺管形成比例、核多形性、核分裂象计数等量化参数，综合计算组织学分级；同时支持自动识别常见组织学类型（如浸润性导管癌、浸润性小叶癌、黏液癌等），并输出其诊断置信度与形态学依据；
- c) 免疫组化定量评分：应支持对 ER、PR、HER2、Ki-67 等免疫组化染色切片进行自动化阳性细胞比例、染色强度及 H-score/Allred 评分计算，辅助判定 HER2（0/1+/2+/3+）和 Ki-67 增殖指数，为分子分型提供客观量化依据；对于 HER2（2+）病例，应自动提示 FISH 检测的必要性。

6.6 治疗方案推荐

乳腺癌辅助诊疗智能体应支持基于患者个体特征提供循证治疗方案推荐：

- a) 方案知识库构建：应支持整合权威指南、最新临床研究、专家共识及未形成指南的前沿证据，构建结构化、可更新的治疗方案知识库（知识库内容包括但不限于 ASCO、ESMO、NCCN、CSCO BC、CACA-CBCS 等国内外主流乳腺癌诊疗指南，以及《中国乳腺癌内分泌治疗专家共识》等共识文件）；
- b) 个性化方案匹配：应支持根据患者精准分期分型、绝经状态、既往治疗反应、体能状态、合并症、经济状况及药物可及性，结合历史相似病例的多维疗效与生存数据，为患者匹配疗效相近的真实世界案例，生成按优先级排序的个体化治疗建议；方案推荐前宜纳入合并症评估（如 Charlson 合并症指数）、老年综合评估（CGA）及多重用药审查（Beers/STOPP 标准），并评

估内分泌治疗与共病的相互作用（芳香化酶抑制剂加重骨质疏松、他莫昔芬致血栓与子宫内膜增厚、内分泌治疗对血糖血脂的影响等）；应支持关键治疗节点（如保乳手术、全乳切除手术、一期乳房重建与二期乳房重建等）的个性化权衡与推荐，充分尊重患者的身体自主权与生活质量诉求；

- c) 方案对比与解释：应支持对不同推荐方案的预期疗效、无病生存期/总生存期数据、常见不良反应与管理措施、费用成本等进行可视化对比，并明确标注方案所依据的指南版本及推荐级别，提供循证依据与机制解释，重点展示不同方案在生存获益、外观保留、功能影响、经济负担及生活质量上的差异，辅助医患共同决策，确保推荐过程公平、透明、可释，充分符合科技伦理原则；
- d) 动态方案调整：应支持基于反馈的真实疗效数据，重新触发个性化方案匹配，生成用药调整建议。

6.7 用药管理

乳腺癌辅助诊疗智能体应支持用药时的查询功能：

- a) 药物信息多渠道查询：应支持用户拍照识别或手动输入药品名称、成分等关键信息进行查询，系统应提供详细的药物信息，包括适应症、用法用量、禁忌反应、副作用、相关保险（医保、商保）政策、不同国家获批适应症等，帮助用户全面了解药品特性；
- b) 个性化用药建议：应支持结合既往病史、用药记录等信息提供个性化的用药建议，如药物使用的注意事项、潜在的药物相互作用风险等，同时应支持导入用药计划，并设置定时用药提醒，辅助用户合理规划、规范执行用药方案。个性化用药建议应支持药物相互作用审查，包括但不限于他莫昔芬经 CYP2D6 代谢与帕罗西汀等 SSRI 类抗抑郁药的相互作用、抗凝药、降糖药及激素类等老年患者常见用药间相互作用；
- c) 药物不良反应监测：应支持对乳腺癌治疗中常见的不良反应建立主动监测与管理机制（如对于高血糖不良反应，应明确检测类型为静脉血浆葡萄糖，检测条件为空腹；显式标注依据 CTCAE v5.0 标准进行高血糖分级——G1 级为 $>$ 正常上限 ~ 8.9 mmol/L，G2 级为 $8.9 \sim 13.9$ mmol/L，G3 级为 > 13.9 mmol/L (> 250 mg/dL)。基线应整合空腹血糖、OGTT、胰岛素、糖化血红蛋白、BMI、腰围、既往史、家族史等多维度指标进行高危分层；治疗中持续监测。空腹血糖 ≥ 8.9 mmol/L ($\geq$ G2 级) 时主动触发内分泌会诊，并提示患者加强监测； $\geq$ G3 级 (> 13.9 mmol/L) 时强制弹窗并触发方案调整）；
- d) 内分泌治疗药物专项管理：应支持对他莫昔芬、芳香化酶抑制剂、CDK4/6 抑制剂等内分泌治疗药物进行专项管理，包括但不限于：长疗程用药依从性监测与提醒、药物相互作用审查及不良反应主动监测。
- e) 内分泌治疗不良反应监测体系：应支持对内分泌治疗相关不良反应的主动监测与管理机制，包括：
 - 1) 芳香化酶抑制剂：应支持基线及治疗后每 1~2 年进行 DXA 骨密度监测，评估骨质疏松及骨折风险，并提示钙剂与维生素 D 补充建议；
 - 2) 他莫昔芬：应支持每年进行妇科超声监测子宫内膜厚度，评估子宫内膜增生或癌变风险；
 - 3) 芳香化酶抑制剂与他莫昔芬：应支持每 6~12 个月进行血脂监测，评估心血管事件风险。

6.8 MDT 多学科会诊支持

乳腺癌辅助诊疗智能体应支持对MDT各环节的协助功能：

- a) 会诊前智能筹备：
 - 1) MDT 病例自动筛选：应支持根据预设规则（如复杂疑难、复发转移、方案争议等临床场景），从医院信息系统中自动识别并抓取待讨论患者，主动提示主管医生发起 MDT；
 - 2) 病例资料自动整理：应支持基于融合与结构化后数据生成预讨论摘要或演示文稿；
 - 3) 指南共识预分发：应支持在 MDT 会诊前自动检索并提取与患者当前情况相关的指南条文及共识要点，提前分发给参与讨论的专家。
- b) 会诊中决策支持：

- 1) 会诊记录智能生成：应支持对讨论过程进行语音实时记录并转为文字，能识别并结构化整理各方意见，生成标准化 MDT 会诊记录；
- 2) 前沿信息支持：应支持检索方案知识库中记录的前沿进展，辅助不同科室医生决策；
- c) 会诊后执行与闭环：
 - 1) 决策提醒与转归知会：应支持根据 MDT 形成的治疗方案，在关键执行节点向主管医生发出提醒，并将患者后续治疗转归知会参与会诊的其他科室医生；
- d) 专病数据库归档：应支持将 MDT 讨论病例结构化记录案专病维度标记归档，形成可供后续科研查询与导出的数据集；
- e) 内分泌代谢联合管理：应支持对合并糖尿病、甲状腺疾病、骨质疏松、代谢综合征等内分泌代谢性疾病的病例，或需进行绝经状态判定、内分泌治疗骨健康管理及代谢副作用管理的病例，强制邀请内分泌科医师参与讨论，并在会诊记录中体现内分泌科意见。

6.9 预后分析

乳腺癌辅助诊疗智能体应支持个体化预后评估：

- a) 多模型集成预测：应支持基于深度学习、机器学习的预测模型，对患者的复发风险、转移风险生存概率等进行综合量化评估，宜支持基于评估结果调整治疗方案；
- b) 关键因素可视化：应支持展示影响患者预后的主要风险因素及其贡献度，如淋巴结转移 ≥ 4 个、三阴性分子亚型、Ki-67 高表达等；
- c) 动态预后更新：应支持在治疗关键节点或获得新数据后，重新进行预后评估，动态反映病情变化对远期结局的影响。

6.10 组学数据分析

乳腺癌辅助诊疗智能体应支持解读多组学数据：

- a) 多组学数据集成：应支持 BRCA1/2、PIK3CA 等乳腺癌相关基因检测数据分析，宜支持乳腺癌相关转录组、蛋白组数据的数据分析。对于 BRCA1/2 基因检测，应区分胚系突变与体细胞突变；若检出胚系致病变异，应提示遗传咨询、家系风险管理及对侧乳腺风险管理等临床建议；
- b) 生物标志物挖掘：应支持能利用生物信息学算法，识别与乳腺癌预后、治疗敏感性相关的突变、通路及特征谱，并关联临床表型；
- c) 临床意义解读：应支持生成组学发现的临床可读性报告，解释其与靶向药物、临床试验或遗传风险的关联，辅助精准医疗决策；
- d) 基因突变智能预测：应支持基于多模态数据（如病理全切片图像与临床结构化数据）对乳腺癌驱动基因（如 PIK3CA 等）突变状态进行智能预测，辅助分子检测前的病例筛选与优先级排序。

6.11 诊后随访

乳腺癌辅助诊疗智能体应实现全周期的规范化诊后随访管理。

- a) 个性化随访计划生成：应支持根据患者的治疗方案、分期分型及预后，自动生成包含随访时间、必查项目、健康指导的定制化计划。随访计划应纳入内分泌治疗依从性随访节点（每 3~6 个月），并根据用药类型设置相应的安全性监测项目，包括芳香化酶抑制剂使用者的骨密度监测（每 1~2 年 DXA）、他莫昔芬使用者的子宫内膜监测（每年妇科超声）及血脂监测（每 6~12 个月）等；
- b) 多渠道随访执行：应支持通过 APP、短信、电话等方式推送随访提醒，并重点收集患侧及对侧乳腺异常症状、放疗区域皮肤与心肺症状、内分泌治疗相关不良反应、靶向治疗心脏毒性等相关反馈数据。随访内容应纳入患者报告结局，包括潮热、关节痛、睡眠障碍、性功能等生活质量指标；
- c) 复发转移监测：应支持对随访中报告的异常症状或检查结果进行自动筛查与预警，确保及时干预。
- d) 疗效动态监测与反馈：应支持收集的随访疗效反馈、不良反应数据及复查结果，动态评估当前治疗方案的获益风险比，并触发动态方案调整；

7 准确性要求

7.1 模型验证规范

模型数据集的训练、验证、测试数据应在患者维度独立划分；名确金标准来源、标注者资质、争议裁决方式；宜开展多中心、跨地域、多机型的外部验证。

7.2 模型比较与统计检验

乳腺癌辅助诊疗智能体涉及的各类指标应支持基于Bootstrap重采样方法计算各评估指标的95%置信区间。

7.3 二分类任务

乳腺癌辅助诊疗智能体涉及的二分类任务包括健康指标（正常、异常）、健康风险（有、无）等。将通过以下指标衡量智能体准确性。

二分类混淆矩阵

分类		人工智能分类	
		阳性	阴性
参考标准分类	阳性	真阳性（TP）	假阴性（FN）
	阴性	假阳性（FP）	真阴性（TN）

a) 灵敏度（Sen）

$$\text{Sen} = \text{TP} / (\text{TP} + \text{FN}) \times 100\%$$

b) 特异度（Spe）

$$\text{Spe} = \text{TN} / (\text{TN} + \text{FP}) \times 100\%$$

c) 准确率（Acc）

$$\text{Acc} = (\text{TP} + \text{TN}) / (\text{TP} + \text{TN} + \text{FP} + \text{FN}) \times 100\%$$

7.4 文书生成类任务

乳腺癌辅助诊疗智能体涉及的文书生成类包括干预建议（根据个人健康评估结果，匹配对应的检测建议）、个性化用药建议、解决方案推荐等，针对此任务，将通过以下指标衡量生成内容与标准答案的区别。

a) ROUGE-N: 对摘要任务，计算客观指标ROUGE-N，其计算公式如下：

$$\text{ROUGE-N} = \frac{\sum_{S \in \{\text{ReferenceSummaries}\}} \sum_{\text{gram}_n \in S} \text{Count}_{\text{match}}(\text{gram}_n)}{\sum_{S \in \{\text{ReferenceSummaries}\}} \sum_{\text{gram}_n \in S} \text{Count}(\text{gram}_n)}$$

式中：

N——即 n-gram，文本内容滑动窗口词元数，参考值为 2；

$\text{Count}_{\text{match}}(\text{gram}_n)$ ——参考摘要和机器生成摘要中共有的 n-gram 的数量；

$\text{Count}(\text{gram}_n)$ ——参考摘要中 n-gram 的数量；

b) 关键词命中率

$$\text{HitRate} = \frac{\text{Count}_{\text{Hit}}}{\text{len}(\text{keyword})} \times 100\%$$

式中：

$\text{Count}_{\text{Hit}}$ ——机器生成文本中命中关键词的数量

$\text{len}(\text{keyword})$ ——关键词的数量

- c) **BERTScore**: 对生成任务, 计算客观指标BERTScore, 计算公式如下:

$$\begin{aligned} sim(x_i, y_i) &= \frac{Emb(x_i) \cdot Emb(y_i)}{\|Emb(x_i)\| \|Emb(y_i)\|} \\ Precision &= \frac{1}{|x|} \sum_{x_i \in x} \max_{y_i \in y} sim(x_i, y_i) \\ Recall &= \frac{1}{|y|} \sum_{y_i \in y} \max_{x_i \in x} sim(x_i, y_i) \\ BERTScore &= \frac{2 \cdot Precision \cdot Recall}{Precision + Recall} \end{aligned}$$

式中:

$Emb(x_i)$ ——句子 x 中词语在经过编码器后的嵌入向量;

$Emb(y_i)$ ——句子 y 中词语在经过编码器后的嵌入向量;

$sim(x_i, y_i)$ ——两词语嵌入向量的余弦相似度;

$Precision$ ——精确率;

$Recall$ ——召回率;

- d) **忠实度**: 衡量模型生成的内容是否忠实于给定的检索证据, 将生成文本分解为多个独立论点后进行计算, 计算公式如下:

$$Faithfulness = \frac{N_v}{N}$$

式中:

N_v ——可被上下文信息证实的论点;

N ——总生成论点。

- e) **Jaccard系数**: 衡量模型生成的决策方案与医生决策方案集合的重叠度, 将生成文本与医生决策方案分解为多个独立论点后进行计算, 计算公式如下:

$$J(A, B) = \frac{|A \cap B|}{|A \cup B|}$$

式中:

A ——生成文本分解后的独立论点集合;

B ——医生决策方案分解后的独立论点集合。

- f) **Recall@K**: 衡量在相关召回条目中, 有多少个在前 K 个召回条目中出现, 计算公示如下:

$$Recall@K = \frac{N_{R-K}}{N_R}$$

式中:

N_{R-K} —— K 个召回条目中相关条目数量;

N_R ——总相关条目数量。

7.5 多分类任务

乳腺癌辅助诊疗智能体涉及的多分类任务为全面指标管理(如血糖、血脂、肝功能等, 对指标异常类型进行多类别判断)、疾病风险评估(如低风险、中风险、高风险)、识别患者的疾病类型、健康干预方案等, 针对此任务, 我们将通过以下指标衡量智能体的准确性。

- a) **Macro-Precision**: 宏精准率

$$Macro - P = \frac{1}{K} \sum_{i=1}^K Precision_i \times 100\%$$

式中:

K——分类任务的总类别数（如三分类时 K=3）

Precision_i——第 i 类精准率，计算公式为 $\text{Precision}_i = \frac{TP_i}{TP_i + \sum_{j \neq i} FP_{j \leftarrow i}}$ （TP_i为 i 类真阳性数，FP_{j←i}为实际非 i 类但预测为 i 类的假阳性数，j≠i 时属于 i 类的误判）

b) Macro-Recall：宏召回率

$$\text{Macro-R} = \frac{1}{K} \sum_{i=1}^K \text{Recall}_i \times 100\%$$

式中：

K——分类任务的总类别数（如三分类时 K=3）

Recall_i——第 i 类召回率，计算公式为 $\text{Recall}_i = \frac{TP_i}{TP_i + \sum_{j \neq i} FN_{i \rightarrow j}}$ （TP_i为 i 类真阳性数，FN_{i→j}为实际 i 类但预测为 j 类的假阴性数，j≠i 时属于 i 类的漏判）

c) Macro-F1：各分类F1分数的算数平均。

7.6 图像类任务

乳腺癌辅助诊疗智能体涉及的图像分割任务为医学影像识别、生理指标图像显示等，针对此任务将通过以下指标衡量智能体的准确性。

a) 准确率(Accuracy)

b) 交并比 (IOU)

$$\text{IOU} = TP / (TP + FP + FN)$$

c) DICE 系数 (DICE)

$$\text{DICE} = 2 * TP / (TP + FP + TP + FN)$$

d) 精确率 (Precision)

$$\text{Precision} = TP / (TP + FP)$$

e) 召回率 (Recall)

$$\text{Recall} = TP / (TP + FN)$$

8 智能体能力要求

8.1 感知能力

8.1.1 知识边界识别

医疗健康行业智能体应具备一定的回答时效性，当推理所依据的信息超出自身训练知识范围、知识库召回知识范围或存在矛盾时，应支持明确识别知识边界，避免产生虚假或无依据的结论。

8.1.2 图像识别能力

医疗健康行业智能体应具备一定的图像识别能力，可判断图像所属模态，并根据图像任务类型选择评价指标，衡量指标如下：

- a) 准确率 (Acc)
- b) 灵敏度 (Sen)
- c) 特异度 (Spe)
- d) 精确率 (Pre)
- e) F1 分数

- f) 交并比 (IOU)
- g) DICE 系数 (DICE)

8.1.3 组学分析能力

医疗健康行业智能体应支持多组学分析能力，可判断数据所属组学并支持基因组学、转录组学、蛋白组学等常见组学的分析与联合分析。

8.1.4 指代消解

医疗健康行业智能体应支持指代消解能力，即多轮对话中某个轮次代词或名词可能指代多种不同事物情况下识别正确。

8.2 规划能力

8.2.1 任务规划

8.2.1.1 目标拆解

医疗健康行业智能体应支持对整体任务进行合理拆解。

- a) 目标识别认知：医疗健康行业智能体应支持对目标进行深入认知，包括但不限于关键信息和潜在障碍。
- b) 目标分析预测：医疗健康行业智能体应支持对目标进行分析预测，包括但不限于目标概念、结构、复杂性、层次、目标间关系等；
- c) 拆解关联度：医疗健康行业智能体应确保子目标间高度关联；
- d) 拆解合理性：医疗健康行业智能体拆解目标时宜参考拆解子目标可行性、依赖关系和优先级，保障目标拆解结果的合理性及可操作性；
- e) 拆解可解释性与可视化：医疗健康行业智能体应支持提供拆解规划方案的详细解释和可视化展示，帮助用户或开发者理解方案的生成过程和结果。

8.2.1.2 规划策略

医疗健康行业智能体应支持任务内或任务间的组织规划。

- a) 规划结构性：应支持按照一定的结构进行任务规划，如线性、分层、并行、树状、网状、条件、迭代等；
- b) 规划逻辑性：应确保子任务之间有明确的逻辑关系；
- c) 规划一致性：在任务间或任务内部组织规划时，应具备规划一致性和协调性，避免重复任务、死循环任务、冲突任务及无效任务等不一致问题；
- d) 冲突解决预案：应具备对内部策略冲突进行预案的能力。在规划阶段应对可能出现的策略冲突节点进行预判并准备合理冲突解决预案；
- e) 高效规划策略：在为了完成指定任务给出的规划步骤中，必要且有效的步骤比例应高于设定阈值。

8.2.2 任务调度

8.2.2.1 调度机制

医疗健康行业智能体应支持多种任务调度机制，具备一定鲁棒性。

- a) 调度机制：应支持根据任务紧急程度、资源占用及依赖关系动态选择调度策略；
- b) 鲁棒性：在面对异常情况时应支持迅速适应并重新规划任务调度，如自动干预及手动干预；
- c) 自主性：应支持自动调度医疗健康行业智能体工作和协同。

8.2.2.2 组织协调

医疗健康行业智能体执行任务时应具有各项组织协调能力。

- a) 资源协调：应支持对时间分配、计算资源管理、数据访问与存储、多源信息整合；
- b) 任务分配：应支持在并发请求场景下，依据实时资源状况，将任务动态分配到不同的处理单元，实现负载均衡；

- c) 进度监控：应支持监控流程执行进度，并对异常情况进行报警；
- d) 应急处置：当紧急事件发生，应支持灵活调整任务分配策略，具备应急能力。

8.3 记忆能力

8.3.1 提示词管理

医疗健康行业智能体应具备提示词管理相关功能。

- a) 提示词模板预设：应支持多种预制的提示词模板，如文本生成类、知识问答类、逻辑推理类等；
- b) 提示词框架预设：应支持多种提示词框架，在不同框架提问下效果稳定；

8.3.2 短期记忆

医疗健康行业智能体应支持记忆尽量多轮次的历史对话：

- a) 历史对话轮次：计算在模型性能没有明显下降的情况下，智能体最长应支持的历史对话轮次应高于 20 轮对话；
- b) 存储容量：单次对话下能够记住和存储的词元数量应高于 10 万。

8.3.3 长期记忆

医疗健康行业智能体应支持长期记忆：

- a) 检索速度：从接收到查询请求到返回检索结果所需的时间应低于 30 秒；
- b) 检索准确：医疗健康行业智能体返回的检索结果与用户查询意图的匹配程度应不低于通用检索方法（如 BM25 等）；
- c) 检索覆盖范围：应支持对时效性要求较高的信息进行及时检索，并明确标识信息的来源及更新时间；
- d) 知识更新：智能体知识更新频次与质量应与医疗行业指南一致；
- e) 忠实度：医疗健康行业智能体基于长期记忆生成的论点应被检索到信息支持；
- f) 记忆隔离：不同患者、不同用户、不同会话之间不得发生信息串扰；
- g) 隐私控制：仅保存完成任务所必要的信息，并支持删除、过期和权限控制；
- h) 自优化功能：应支持存储操作记忆与日志，能记录与统计不同功能模块的点击率、使用时长及用户采纳率，基于真实使用数据实现功能的优化。

8.4 执行能力

8.4.1 临床推理

医疗健康行业智能体应支持基于患者多维度数据（分型、分期、生物标志物、既往治疗反应等）进行临床推理，包括但不限于鉴别诊断、治疗路径推演、风险因素关联分析。

8.4.2 虚拟环境执行

医疗健康行业智能体在虚拟环境下应具备虚拟环境执行能力。

- a) 工具调用：应支持调用外部工具如文档解析、语音识别、数据库访问、图像识别、HIS/LIS/PACS 接口等并完成特定任务；
- b) 执行容错与回退机制：应具备处理操作失败等异常情况的能力，能进行错误提示、启动备选方案或安全回退，并记录故障信息；
- c) 权限与执行边界：应支持不同工具应按照风险等级进行权限控制。涉及医嘱、处方、治疗方案变更等临床行为，不应未经医师确认直接执行；
- d) 执行可追溯性：应支持记录任务规划、工具调用、输入参数、调用结果、模型输出、人工确认和异常处理等关键过程。

9 易用性要求

9.1 可理解性

9.1.1 语言表达清晰程度

医疗健康行业智能体界面文字、提示及交互内容应简洁准确，避免歧义。对于超出智能体知识边界或数据不足以支撑结论的情况，系统应支持在输出中明确标识知识边界，主动拒答或声明无法提供有效建议，不应生成无依据的回复。

9.1.2 辅助理解手段

医疗健康行业智能体涉及复杂医学知识、操作流程等操作宜辅以图文与循证医学证据展示；关键环节宜设引导提示，提升信息理解效率。

9.2 易学性

9.2.1 帮助文档完整性

医疗健康行业智能体应配备结构化帮助文档，含功能说明、操作指南及常见问题解答，支持关键词检索，内容随平台更新同步修订。

9.2.2 差错信息易理解性

医疗健康行业智能体操作错误或系统异常时，差错信息应明确原因并提供解决方案，不应以技术代码表述。

9.3 易操作性

9.3.1 一键调用功能

医疗健康行业智能体应支持对医院信息化系统（如HIS、LIS、PACS）的集成与调用，避免用户在多个平台间切换。

9.3.2 操作一致性

医疗健康行业智能体各功能模块操作逻辑、交互样式应保持统一，降低用户学习成本。

9.3.3 消息明确性

- a) 医疗健康行业智能体向用户推送的各类消息，如检查提醒、复诊通知、用药提示等，内容应明确具体，包含关键信息，如时间、地点、注意事项等。
- b) 医疗健康行业智能体向用户推送的各类消息的标题和正文应简洁明了，不应使用冗长复杂的表述。
- c) 医疗健康行业智能体消息推送应具备合理的频率和时机，不应过度打扰用户。

9.3.4 辅助输入手段

医疗健康行业智能体应支持智能联想、语音、手写等多种输入方式。

9.3.5 功能开关

医疗健康行业智能体应提供对于设计用于提升诊疗质量上限的功能（非保障医疗安全底线的强制性功能）的开关选项，允许医生根据个人工作习惯和临床需要自由启用或关闭，避免增加临床工作负担。

10 安全性要求

10.1 基础设施安全

10.1.1 硬件设备安全性

医疗健康行业智能体涉及的硬件设备（如网络设备、存储设备、计算设备等）的安全防护能力应包含：

a) 通用安全要求：

- （1）应满足物理安全保障要求，包含防火、防雷、防水、灾备、授权等；
- （2）应满足功能安全保障要求，包含设备标签、硬件接口安全、固件安全、驱动程序安全等；
- （3）应满足管理安全保障要求，包含管理机制、管理人员等；

b) 网络设备安全专用要求：分布式训练、推理时应满足组网安全保障要求，包含网络带宽、网络时延、网络丢包率、网络抖动等；

c) 计算设备安全专用要求：

（1）应具备保障人工智能加速芯片应具安全保障能力，包含 AI 加速芯片信息窃取防护、架构安全漏洞防护等；

（2）应具备保障人工智能加速芯片在异构场景下应具备稳定运行的能力，包含 CPU 与 GPU 相结合的场景；

（3）应具备保障人工智能加速芯片运行环境安全的能力。

10.1.2 软件设备安全性

医疗健康行业智能体应支持多种设施如依赖库、AI 框架、向量数据库、中间件、接口等具备安全防护能力，包含：

a) 漏洞管理：软件设施应定期进行漏洞扫描和修复，具备完善的漏洞响应机制；

b) 安全更新：软件设施应及时更新安全补丁，以防止新出现的安全威胁。

10.2 数据安全

医疗健康行业智能体应支持数据采集、数据预处理、数据使用等数据相关内容具备安全防护能力，包含存储安全、隐私保护、过程安全、销毁安全等。在调用历史相似病例数据进行疗效对比时，应确保所有参照数据均已进行脱敏处理，涉及患者个人信息的数据处理应符合 GB/T 35273-2020 及伦理要求，并根据适用情形履行告知、授权或其他合法性要求。

10.3 应用安全

10.3.1 内容安全

医疗健康行业智能体输出内容（含生成内容、决策内容）应符合全人类普适的道德伦理及医学伦理要求。

- a) 应支持尊重人权，包括医疗健康行业智能体输出内容（含生成内容、决策内容）应遵循人权的普遍性和不可侵犯性的原则，尊重人类平等、尊严和自由的权利；
- b) 应支持公平与非歧视性，包括医疗健康行业智能体输出内容（含生成内容、决策内容）避免产生偏见及歧视性结果的程度；
- c) 应符合科技伦理原则，包括增进人类福祉、坚持公平公正、推动透明可释、确保可控可信等；
- d) 应遵循科技伦理指标，包括公平性、透明可释性、数据隐私、可控可靠性、内容向善、责任可追溯、可持续性等。

10.3.2 服务安全

医疗健康行业智能体应支持服务安全可信、内容安全可信等应用相关内容具备安全防护能力,包含:

- a) 服务安全: 应满足模型安全保障要求, 包含 MTTF、服务安全性、服务合规性、反馈处置机制等;
 - b) 记忆自优化提醒: 基于真实数据实现自优化与系统更新后应支持通过明确的通知机制确保用户知晓。
-

