ICS
CCS

团　　体　　标　　准

T/ISC XXXX—XXXX

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 intelligent agent in the healthcare industry

（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。

XXXX - XX - XX 发布　　XXXX - XX - XX 实施

中国互联网协会　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。

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提出并归口。

本文件起草单位：

本文件主要起草人：

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。

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）

5 CT：计算机断层扫描（Computed Tomography）总体要求

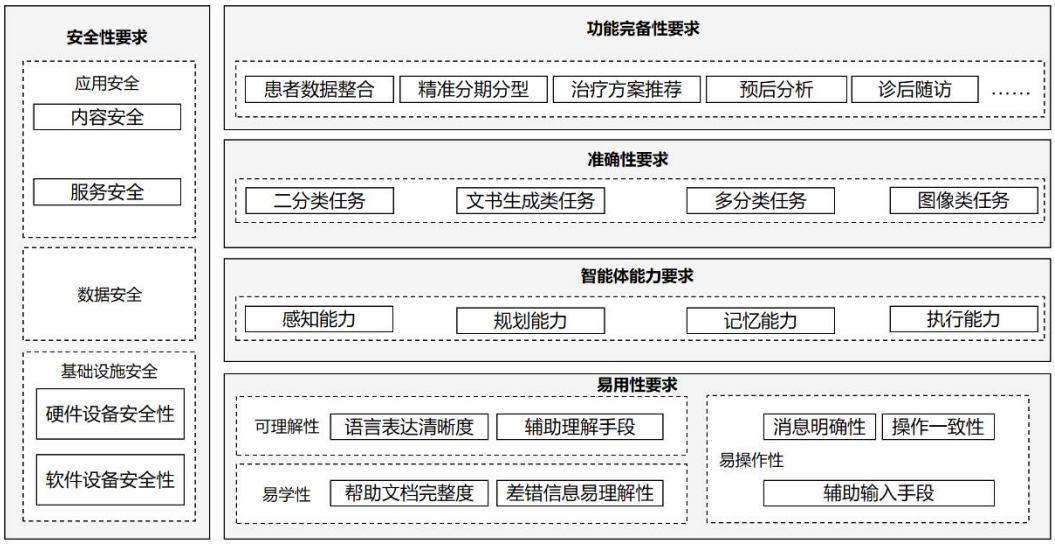

图 1　乳腺癌辅助诊疗智能体的架构示意图

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，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；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。

6　功能完备性技术要求

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：

a) 多模态数据接入：应支持集成来自院内信息系统（如 HIS、LIS、PACS）、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；

b) 数据融合与结构化：应利用自然语言处理、图像识别等技术，从异构数据源中自动提取乳腺病灶的 BI-RADS 分类、病理组织学类型与分级、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、时序性的患者数据全景视图；

c) 质量校验与补全：应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等，基于医学知识图谱或算法模型提示补全建议，为后续分析提供可靠数据基础。

6.2　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：应内置 TNM 等国际国内主流分期标准，并能根据病理、影像、临床检查结果，自动计算并推荐分期，同时对比展示不同标准下的结果；

b) 分子分型智能判别：应结合 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、三阴性等分子亚型，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；

c) 动态更新与回溯：当患者出现新发转移或复发时，应能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。

6.3 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：应整合权威指南、最新临床研究及专家共识，构建结构化、可更新的治疗方案知识图谱；

b) 个性化方案匹配：应根据患者精准分期分型、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；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：应能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。。

6.4 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，宜支持乳腺癌相关转录组、蛋白组数据的导入、标准化存储与管理；

b) 生物标志物挖掘：应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：应提供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。

6.5 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：应基于深度学习模型，对乳腺 X 线、超声、MRI 及 CT 影像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) 特征提取与预后关联：应能提取影像组学特征，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。

6.6 预后分析

乳腺癌辅助诊疗智能体应能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、生存概率等进行综合量化评估；

b) 关键因素可视化：应清晰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：应能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。

6.7 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；

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；

c) 复发转移监测：应特别关注复发转移的早期迹象，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) 疗效动态评估与方案调整： 应基于随访收集的疗效反馈、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；当出现疾病进展、严重不耐受或新药/新方案上市等情况时，应智能提示调整后续治疗策略与随访方案，实现从“静态方案推荐”向“动态闭环管理”的演进，确保患者全程获得适时、适宜的个体化照护。

6.8 药物查询

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：用户可通过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、副作用等，帮助用户全面了解药品特性；

b) 个性化用药建议：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。

7 准确性要求

7.1 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）

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

b) 特异度（Spe）

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

c) 准确率（Acc）

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

7.2 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：

$$\mathrm{ROUGE-N}=\frac{\sum S\in\{\mathrm{ReferenceSummaries}\}\sum \mathrm{gram_n}\in \mathrm{sCount_{match}(gram_n)}}{\sum S\in\{\mathrm{ReferenceSummaries}\}\sum \mathrm{gram_n}\in \mathrm{sCount(gram_n)}}$$

式中：

N——即 n-gram，文本内容滑动窗口字节数，参考值为 2；

$\mathrm{Count_{match}(gram_n)}$——参考摘要和机器生成摘要中共有的 n-gram 的数量；

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

b) 关键词命中率

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

式中：

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

len(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：

$$sim(x_i, y_i) = \frac{Emb(x_i) \cdot Emb(y_i)}{\| Emb(x_i) \| \| Emb(y_i) \|}$$

$$Precision = \frac{1}{|x|} \sum_{x_i \in x} \max_{y_i \in y} sim(x_i, y_i)$$

$$Recall = \frac{1}{|y|} \sum_{y_i \in y} \max_{x_i \in x} sim(x_i, y_i)$$

$$BERTScore = \frac{2 \cdot Precision \cdot Recall}{Precision + Recall}$$

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；

7.3 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

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

式中：

K——分类任务的总类别数（如三分类时 K=3）

$\mathrm{Precision_i}$——第 i 类精准率，计算公式为$\mathrm{Precision_i} = \frac{\mathrm{TP_i}}{\mathrm{TP_i} + \sum_{\mathrm{j} \neq \mathrm{i}} \mathrm{FP_{j \leftarrow i}}}$（$\mathrm{TP_i}$为 i 类真阳性数，$\mathrm{FP_{j \leftarrow i}}$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

$$\mathrm{Macro-R} = \frac{1}{\mathrm{k}} \sum_{\mathrm{i}=1}^{\mathrm{K}} \mathrm{Recall_i} \times 100\%$$

式中：

K——分类任务的总类别数（如三分类时 K=3）

$\mathrm{Recall_i}$——第 i 类精准率，计算公式为$\mathrm{Recall_i} = \frac{\mathrm{TP_i}}{\mathrm{TP_i} + \sum_{\mathrm{j} \neq \mathrm{i}} \mathrm{FN_{i \rightarrow j}}}$（$\mathrm{TP_i}$为 i 类真阳性数，$\mathrm{FN_{i \rightarrow j}}$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：宏精准率与宏召回率的调和平均

$$\text{Macro}-\text{F1}=\frac{2\times\text{Macro}-\text{P}\times\text{Macro}-\text{R}}{\text{Macro}-\text{P}+\text{Macro}-\text{R}}$$

7.4 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）

$$IOU=TP/(TP+FP+FN)$$

c) DICE 系数（DICE）

$$DICE=2*TP/(TP+FP+TP+FN)$$

d) 精确率（Precesion）

$$Precesion = TP/(TP+FP)$$

e) 召回率（Recall）

$$Recall = TP/(TP+FN)$$

8 智能体能力要求

8.1 感知能力

8.1.1 回答时效性

医疗健康行业智能体应具备一定的回答时效性。

通过用户从发起请求到系统或应用程序返回结果的时间计算响应实时性，计算方式如下：

$$ES\_T = R\_T_{finish} - R\_T_{start}$$

式中：

ES_T ——响应时间；

R_T_{finish} ——医疗健康行业智能体返回结果的时间；

R_T_{start} ——用户发起请求的开始时间。

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，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）

$$Pre=TP/(TP+FP)\ x\ 100\%$$

e) F1分数

$$F1=2\times(Pre\times Sen)/(Pre+Sen)$$

8.1.3 推理能力

8.1.3.1 指代消解

医疗健康行业智能体在指代消解能力上应具备一定的准确率。

计算对话系统的指代消解准确率，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。计算公式如下：

$$P_M = \frac{m}{M} \times 100\%$$

式中：

P_M——本轮指代消歧平均准确率；

m ——本轮中每个代词或名词短语被正确识别的次数；

M ——本轮中所有代词或名词短语数量。

8.1.3.2 知识推理

医疗健康行业智能体在知识推理能力上应具备一定的准确率。

根据推理总数和推理正确数，计算F1值：

$$F1 = \frac{2 \times P \times R}{P + R}$$

式中：

P——预测正确的数量/预测出的总数量；

R——预测正确的数量/实际总数量。

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在目标拆解能力上具备一定的性能优越度。

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，保障拆解目标及可操作性；
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：支持按照一定的结构的任务结构进行任务规划，如线性、分层、并行、树状、网状、条件、迭代等；
b) 规划逻辑性：医疗健康行业智能体拆解任务的合理性，确保子任务之间有明确的逻辑关系；
c) 规划一致性：医疗健康行业智能体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；
a) 冲突解决预案：智能体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；
d) 规划策略准确率：即智能体为了完成指定任务给出的规划步骤中，有多少步骤是必要的有效步骤。计算公式如下：

$$E_P = \frac{R_1}{R} \times 100\%$$

式中：

E_p——规划策略准确率；

R_1——完成指定任务所提供的规划策略中有效的操作数量；
R——完成指定任务提供的规划策略中总的操作数量；

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：医疗健康行业智能体调度机制的可选度，如先来先服务、短作业优先、轮转调度机制、优先级调度机制、最早截止时间优先等；
b) 鲁棒性：医疗健康行业智能体在面对异常情况时应能够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：系统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：医疗健康行业智能体对时间分配、计算资源管理、数据访问与存储、多源信息整合的支持度；
b) 任务分配：医疗健康行业智能体应在并发请求场景下，智能体应能依据实时资源状况，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：医疗健康行业智能体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，医疗健康行业智能体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 短期记忆能力

医疗健康行业智能体应具备提示词管理相关功能。

a) 模板丰富度：医疗健康行业智能体应具备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) 框架丰富度：医疗健康行业智能体应支持的提示词框架丰富度，即在不同框架提问下效果稳定，如 ICIO 框架、CRISPE 框架、BROKE 框架等；
c) 模板管理：医疗健康行业智能体应具备提示词模板管理功能，如创建、修改、删除等；

8.3.2 长期记忆能力

8.3.2.1 记忆存储

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，医疗健康行业智能体最长可以支持的历史对话轮次；
b) 知识更新：医疗健康行业智能体知识更新频次与质量；
c) 存储容量：能够记住和存储的长期痕迹字符数量。

8.3.2.2 快速检索

医疗健康行业智能体应支持快速检索功能。

a) 检索速度：医疗健康行业智能体从接收到查询请求到返回检索结果所需的时间；
b) 检索准确性：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；
c) 检索覆盖范围：医疗健康行业智能体能够检索到的信息来源和类型。

8.4 执行能力

8.4.1 虚拟环境执行能力

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) 交互积极性：医疗健康行业智能体的交互积极性，应可以从被动服务向主动服务转变；

b) 交互对象多样性：医疗健康行业智能体与软件环境中的其他实体进行交互的支持度，其他实体包括其他智能体、系统、环境本身等；
c) 数据格式多样性：医疗健康行业智能体需要对接收到的软件环境信息进行理解和解码的能力，环境数据包括文本及多模态数据；
d) 工具丰富度：医疗健康行业智能体可以调用外部工具的数量，如文档解析、语音识别、数据库访问、图像识别等。
e) 执行容错与回退机制：智能体在执行过程中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。

8.4.2 执行能力准确率

a) 计算执行能力准确率，即智能体为了完成指定任务给出的规划步骤中，有多少步骤执行后得到了正确的结果。计算公式如下：

$$P_P = \frac{C_1}{C} \times 100\%$$

式中：
P_p——执行能力准确率；
C_1——完成指定任务所提供的规划策略中得到正确结果的操作数量；
C——完成指定任务提供的规划策略中总的操作数量。

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。

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 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。

9.3.2 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。

9.3.3 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。

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备通用安全保障能力，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，并在数据使用前向患者明确告知数据用途，保障患者的知情同意权。

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) 应支持无偏见歧视性，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：医疗健康行业智能体涉及的模型安全性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。