

# 团体标准

T/GDWJ XXXX—XXXX

## 大语言模型在患者智能交互中应用技术规范

Technical standards for applying large language models in patient  
intelligent interaction

(征求意见稿)

XXXX—XX—XX 发布

XXXX—XX—XX 实施

广东省卫生经济学会发布



## 目 次

前 言 .....	II
引 言 .....	III
大语言模型在患者智能交互中应用技术规范 .....	4
1 范围 .....	4
2 规范性引用文件 .....	4
3 术语和定义 .....	4
3.1 .....	4
3.2 .....	4
3.3 .....	5
3.4 .....	5
4 缩略语 .....	5
5 应用场景 .....	5
5.1 诊前交互 .....	5
5.2 诊中指引 .....	5
5.3 诊后管理 .....	6
6 技术路线 .....	6
6.1 基于多场景交互的深度语义理解增强技术 .....	6
6.3 基于用户档案和医学知识的医疗健康交互技术 .....	7
6.4 自然语言处理（NLP） .....	7
6.5 多模态数据处理 .....	8
6.6 强化学习 .....	8
6.7 隐私保护与数据安全 .....	8
6.8 实时监控与反馈 .....	8
7 应用过程 .....	8
7.1 数据收集与预处理 .....	8
7.2 模型选择与微调 .....	9
7.3 性能评估与验证 .....	9
7.4 部署与应用 .....	9
7.5 伦理与法规遵循 .....	9
7.6 安全与风险管理 .....	9
（资料性） .....	10
参 考 文 献 .....	11

# 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。

请注意本文体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。

本文件由广东省卫生经济学会提出并归口。

本文件起草单位：广州医科大学附属第五医院、讯飞医疗科技股份有限公司、广东省卫生经济学会、东莞市卫生统计信息中心、暨南大学附属顺德医院、中山大学附属口腔医院、中山大学附属第一医院、中山大学附属第三医院、中山大学附属第五医院、南方医科大学附属第三医院、广州医科大学附属第二医院、广州医科大学附属妇女儿童医疗中心、广东省省第二中医院黄埔医院、白云区妇幼保健院。

本文件主要起草人：XXXXXX。

## 引 言

随着技术的不断进步和应用场景的拓展，大语言模型将在医疗领域发挥越来越重要的作用，为患者提供更加优质、高效和便捷的医疗服务。

本文件旨在促进大语言模型在医疗场景中的高效应用，提升医疗服务效率和服务质量，提高患者满意度。

本文件为规范大语言模型在医疗行业的的应用技术要求，包括应用场景、技术路线、应用过程等维度的要求。

文件适用于指导各类医疗机构及相关企业开展基于大语言模型进行本标准主要为大语言模型在患者智能交互中的应用提供规范性指引。

如有未尽事项，或相关事项因立法、法律修改等事由在法律法规等规范文件中另有规定的，应依法遵循相关法律法规规定。

# 大语言模型在患者智能交互中应用技术规范

## 1 范围

本标准规定了基于大语言模型在患者智能交互中的应用场景、过程、技术路线等内容。

本标准适用于医疗机构、卫生主管部门、研究机构、企业等，在患者智能交互中的应用场景的建设、应用和管理等。

## 2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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。

《国务院办公厅关于促进和规范健康医疗大数据应用发展的指导意见》（国办发〔2016〕47号）

《新一代人工智能发展规划》（国发〔2017〕35号）

《关于印发进一步改善医疗服务行动计划（2018-2020年）考核指标的通知》（国卫办医函〔2018〕894号）

《国务院办公厅关于促进“互联网+医疗健康”发展的意见》（国办发〔2018〕26号）

《医院智慧服务分级评估标准体系（试行）》（国卫办医函〔2019〕236号）

《关于深入推进“互联网+医疗健康”“五个一”服务行动的通知》（国卫规划发〔2020〕22号）

《关于推动公立医院高质量发展的意见》（国办发〔2021〕18号）

《关于加快场景创新以人工智能高水平应用促进经济高质量发展的指导意见》（国科发规〔2022〕199号）

《“十四五”全民健康信息化规划》（国卫规划发〔2022〕30号）

《关于开展改善就医感受提升患者体验主题活动的通知》（国卫医政发〔2023〕11号）

《“数据要素×”三年行动计划（2024—2026年）》

《生成式人工智能服务管理暂行办法》（国家互联网信息办公室等令15号）

《医疗健康行业大模型应用技术要求》

## 3 术语和定义

### 3.1

**大语言模型** Large Language Model

是一种基于海量文本数据训练的深度学习模型，能够生成自然语言文本并深入理解文本含义，处理各种自然语言任务，如文本摘要、问答、翻译等。

### 3.2

**自然语言处理** Natural Language Processing

是计算机科学和人工智能领域的一个重要研究方向，它旨在使计算机能够理解、解释和生成人类语言。

### 3.3

#### 医学知识图谱 Medical Knowledge Graph

是一种基于医学领域知识构建的知识库，它通过将医学领域的各种信息和数据进行整合、加工和组织，形成一个结构化、可视化的知识网络。

### 3.4

#### 多模态 Multimodal

是指同时使用多种感官或信息通道来处理和理解信息的能力和现象。在计算机科学和人工智能领域，多模态通常指的是结合文本、图像、音频等多种数据类型进行综合分析和处理的技术。

## 4 缩略语

下列缩略语适用于本文件。

LLM:大语言模型(Large Language Model)

NLP:自然语言处理(Natural Language Processing)

## 5 应用场景

大语言模型（LLM）在医疗领域的应用正逐步深入，覆盖了多个应用场景。本指南主要围绕大语言模型在患者诊前、诊中、诊后的智能交互场景展开论述。

### 5.1 诊前交互

大语言模型在患者诊前交互场景，基于自然语言处理技术与多模态交互技术，模拟医患多轮交互，实现：

a) 应支持基于多轮交互数据，自动提取并生成患者的基本信息和历史病历资料，形成患者画像，实现初步的病情评估和精准的导医导诊。

b) 应支持基于大语言模型的健康咨询服务，如疾病预防、健康管理等方面的问题，提高患者的健康意识和自我管理能力。

### 5.2 诊中指引

大语言模型在患者诊中交互场景，基于通过文档解析、大数据存储、自然语言语义理解等技术，实现：

a) 应支持就诊全流程的消息指引。

- b) 应支持检查、检验报告的解读。
- c) 应支持模拟人工客服提供 7 X 24 小时 AI 客服服务, 精准识别患者的咨询问题, 理解用户意图, 为患者提供准确回复。

### 5.3 诊后管理

大语言模型在患者诊后管理场景, 基于根据患者病情, 提供满意度调查、随访管理、康复方案指导、健康宣教及在线咨询, 辅助患者合理完成康复计划。

- a) 应支持对患者发起自动、批量满意度调查, 并自动进行结果汇总统计。
- b) 应支持自动生成并执行随访计划, 收集患者的康复情况和反馈意见。
- c) 应支持根据患者病情, 动态生成个性化康复方案。
- d) 应支持向患者提供关于疾病、治疗、康复等方面的宣教指导。
- e) 应支持实时在线回复患者在康复过程中的咨询问题。
- f) 应支持协助患者安排后续的医疗预约, 包括复查、专科咨询等。

## 6 技术路线

### 6.1 基于多场景交互的深度语义理解增强技术

以结构化的专业医疗知识体系为基础, 结合背景信息的上下文识别增强技术, 通过结合业务背景信息及对话历史信息, 使用多层注意力机制, 增强系统识别上下文中复杂语义表述的能力。提高对话系统在追踪对话上下文和识别用户意图方面的准确度, 达到准确选用合适的医学知识信息, 使系统可以提供相关性强、针对性高的回答。

### 6.2 面向医疗场景的检索增强型大模型技术

利用外部权威知识库来增强 LLM 的生成质量, 主要包括检索、生成、增强三个层次:

检索(Retrieval): 从外部知识库中检索与输入相关的知识;

生成(Generation): 接收原始输入和检索结果, 输出对应的自然语言文本;

增强(Augmentation): 连接检索和生成, 将检索知识集成到生成模块。

- a) 支持知识存储类型: txt、doc、pdf、excel、xml 接口。
- b) 支持段落切分和向量化存储: 将上传的业务知识按照最优的策略, 自动完成段落切分和向量化存储, 同时开发段落切分参数供调试选择。
- c) 检索技术: 支持向量检索、语义检索、全文检索和混合检索等检索策略。



- d) 检索集成生成：检索信息支持按照不同的权重比例输入至医学大模型中，赋予它查阅外部信息的能力，缓解大模型幻觉和内部知识过时等固有局限性。
- e) 结果溯源：生成结果支持溯源到业务知识段落。

### 6.3 基于用户档案和医学知识的医疗健康交互技术

采用基于用户档案和医学知识的医疗健康交互技术，提升用户个性化交互能力。

- a) 支持基于患者病情画像，调用医学知识插件检索相关的医学知识库。利用大语言模型进行文本语义表征，并通过 GCN 模型对相关医学知识进行编码，获取各信息的向量表示。采用多模型编码，通过底层模型参数共享和各类信息间的 attention 机制，获取最终表示特征，经过全连接层分别输出当前辅检及处置建议。
- b) 结合医疗专家知识的交互路径强化学习技术，实现大语言模型主被动自由切换。在医学知识图谱的基础上，整合各科专家的医疗经验、最新临床实践案例，构建医疗交互事例图谱，构建起专家级的逻辑链。
- c) 结合交互事例图谱、个性化医学知识推荐的输出和专家 Prompt 提示学习训练专家奖励模型，融合医疗专家的知识与学习专家建议去改善算法的预测效果。
- d) 通过近端策略优化（PPO）在交互过程中不断调整大模型的行为策略，迭代优化直至其行为接近真实医疗专家，实现与患者自然的交流，给出专业和个性化建议。

### 6.4 自然语言处理（NLP）

自然语言处理是实现患者与 AI 智能交互的核心技术，使模型能够理解患者的自然语言输入，并生成自然、流畅的回复。

- a) 语言理解：使用预训练语言模型，理解患者的症状描述、病史记录等文本信息。通过大规模语料库训练，能够捕捉复杂的语言结构和语义信息。
- b) 对话管理：通过对话系统管理对话流程，跟踪对话状态，管理上下文信息，确保对话的连贯性和逻辑性。
- c) 情感分析：通过情感分析技术，识别患者的语气和情感状态，以便提供更加人性化和个性化的支持。

## 6.5 多模态数据处理

大语言模型在患者智能交互中须支持处理和整合多模态数据，支持患者通过多种方式（如文本、语音、图像等）与AI进行交互。

## 6.6 强化学习

通过强化学习技术，使大语言模型在与患者的交互过程中不断优化其决策策略，提高服务质量。

- a) 对话优化：通过强化学习算法优化对话策略，使模型能够根据患者的反馈不断改进其回复，提高模型的推理质量、准确性与可靠性。
- b) 个性化推荐：通过强化学习算法，根据患者的个体特征和历史记录，提供个性化的治疗建议和健康管理方案。

## 6.7 隐私保护与数据安全

在患者与AI智能交互过程中，保护患者的隐私和数据安全是至关重要的。

- a) 数据加密：对传输和存储的数据进行加密，确保数据在传输过程中不被窃取或篡改。
- b) 差分隐私：通过添加噪声等方式，保护个体数据的隐私，同时保持数据的整体统计特性。
- c) 联邦学习：在多个设备或机构之间进行分布式训练，每个设备只上传模型参数的更新，而不上传原始数据，从而保护数据隐私。

## 6.8 实时监控与反馈

为了确保交互过程的顺利进行，大语言模型需要具备实时监控和反馈机制。

- a) 实时监控：通过实时监控患者的输入和模型的输出，确保交互过程的准确性和连贯性。
- b) 用户反馈：通过收集用户的反馈信息，不断优化模型的性能和用户体验。

# 7 应用过程

大语言模型（LLM）在医疗场景应用的应用过程涉及数据收集、模型训练、性能评估、部署与应用等多个环节。

## 7.1 数据收集与预处理

- a) 数据多样性：确保收集的数据涵盖广泛的医学领域，包括病历记录、医学文献、交互数据等。
- b) 数据质量：进行严格的数据清洗和预处理，去除噪声和无关信息，提高数据的质量和一致性。
- c) 隐私保护：在数据收集过程中严格遵守患者隐私保护法规，如《个人信息保护法》等。

## 7.2 模型选择与微调

- a) 模型架构：选择适合医疗领域的大语言模型架构，如 Transformer、BERT、GPT 等，并根据具体需求进行微调或开发新的模型架构。
- b) 指令微调：针对特定医疗任务进行指令微调，以提高模型的性能和准确性。
- c) 跨领域适应：考虑模型在不同医疗场景下的适应性，如导诊分诊、病情分析、患者咨询等。

## 7.3 性能评估与验证

- a) 基准测试：构建涵盖多个医疗问答数据集的基准测试，以评估模型的临床知识和问答能力。
- b) 专家评估：邀请医学专家参与模型性能的评估，确保模型输出的准确性和可靠性。
- c) 持续迭代：根据评估结果对模型进行迭代优化，不断提高模型的性能和泛化能力。

## 7.4 部署与应用

- a) 系统集成：将训练好的模型集成到患者交互类医疗信息化系统中。
- b) 实时更新：随着医疗领域知识的不断更新和变化，定期收集新的医疗文本数据，并对模型进行更新和优化。

## 7.5 伦理与法规遵循

- a) 透明度：确保模型的决策过程透明可解释，以便医生和监管机构理解和信任模型的输出。
- b) 公平性：避免模型在处理不同患者群体时产生偏见或歧视。
- c) 法规遵循：严格遵守医疗行业相关的法律法规和伦理准则，确保模型的合法合规应用。

## 7.6 安全与风险管理

- a) 错误检测与纠正：建立机制来检测和纠正模型可能产生的错误输出或幻觉。
- b) 风险评估与管理：对模型在医疗场景中的潜在风险进行全面评估和管理，确保患者安全。
- c) 应急响应计划：制定应急响应计划以应对可能出现的突发情况或系统故障。

## 附 录 A

（资料性）

## 参 考 文 献

- [1] 《国务院办公厅关于促进和规范健康医疗大数据应用发展的指导意见》（国办发〔2016〕47号）
  - [2] 《新一代人工智能发展规划》（国发〔2017〕35号）
  - [3] 《关于印发进一步改善医疗服务行动计划（2018-2020年）考核指标的通知》（国卫办医函〔2018〕894号）
  - [4] 《国务院办公厅关于促进“互联网+医疗健康”发展的意见》（国办发〔2018〕26号）
  - [5] 《医院智慧服务分级评估标准体系（试行）》（国卫办医函〔2019〕236号）
  - [6] 《关于深入推进“互联网+医疗健康”“五个一”服务行动的通知》（国卫规划发〔2020〕22号）
  - [7] 《关于推动公立医院高质量发展的意见》（国办发〔2021〕18号）
  - [8] 《关于加快场景创新以人工智能高水平应用促进经济高质量发展的指导意见》（国科发规〔2022〕199号）
  - [9] 《“十四五”全民健康信息化规划》（国卫规划发〔2022〕30号）
  - [10] 《关于开展改善就医感受提升患者体验主题活动的通知》（国卫医政发〔2023〕11号）
  - [11] 《“数据要素×”三年行动计划（2024—2026年）》
  - [12] 《生成式人工智能服务管理暂行办法》（国家互联网信息办公室等令15号）
  - [13] 《医疗健康行业大模型应用技术要求》
-