AI HEALTH PRODUCT WORKFLOW & PROMPT DESIGN

AI体检报告解读与健康行动助手

AI工作流与Prompt设计文档 v1.0

AI能力拆解 · Prompt体系 · RAG知识库 · 医疗安全 · 数据流 · MVP落地

产品类型： AI健康产品 / 体检报告解读工具 / 健康行动管理助手

文档用途： AI产品工作流设计 / Prompt设计 / 作品集项目资料

版本日期： 2026年6月

文档信息

项目	内容
文档名称	《AI体检报告解读与健康行动助手 AI工作流与Prompt设计文档》
产品名称	AI体检报告解读与健康行动助手
文档类型	AI产品工作流设计文档 / Prompt设计文档 / AI能力说明文档
版本	v1.0 整合版
日期	2026年6月
产品类型	AI健康产品 / 体检报告解读工具 / 健康行动管理助手
适用阶段	原型设计、MVP开发、AI能力设计、作品集展示

重要说明

本产品中的 AI 不定位为医生、诊断系统、处方工具或治疗方案生成器。

本产品中的 AI 定位为：健康信息解释助手、体检报告结构化助手、异常指标说明助手、健康行动建议助手、医疗安全提示助手、健康档案摘要助手。

本文件重点说明：AI 如何嵌入体检报告解读产品流程，如何设计 Prompt，如何控制医疗风险，如何使用知识库与上下文，如何评估 AI 输出质量，以及如何让 AI 能力成为一个可落地、可审核、可迭代的产品系统。

目录

1. 文档基础信息
2. AI产品定位与设计原则
3. AI整体工作流设计
4. AI能力模块设计
5. Prompt设计方法论
6. Prompt模板设计
7. 医疗安全与Prompt风险控制
8. RAG与医学知识库设计
9. 数据流与上下文管理
10. AI输出质量评估
11. AI异常处理与降级策略
12. MVP阶段AI实现方案
13. 技术协作与产品交付说明
14. 作品集展示角度
15. 文档结论

0. 文档基础信息

0.1 文档目的

本文件的目的，是系统说明《AI体检报告解读与健康行动助手》中的 AI 能力如何被设计、拆解、约束、调用、审核和评估。

本产品不是简单地在页面中接入一个大模型聊天框，也不是让用户随便向 AI 提问健康问题。它的核心设计思路是：将 AI 能力拆解到体检报告解读的完整业务流程中，让 AI 在结构化数据、规则判断、医学知识库、安全审核和用户交互之间发挥作用。

本文件重点回答以下问题：

- AI 在本产品中的定位是什么？
- AI 可以做什么，不能做什么？
- AI 如何参与体检报告上传、识别、结构化、解读、行动建议和追问？
- 哪些任务适合规则处理，哪些任务适合大模型处理？
- Prompt 如何设计，才能保证输出稳定、安全、可控？
- AI 输出如何经过医疗安全审核？
- 如何避免 AI 诊断、AI 处方、AI 恐吓和 AI 幻觉？
- 如何评估 AI 输出质量？
- MVP 阶段 AI 能力应如何分阶段实现？
- 这套 AI 设计如何展示为 AI 产品经理作品集能力？

0.2 关联文档

文档	作用
产品分析报告	回答为什么做、机会在哪里
PRD产品需求文档	回答具体怎么做、做哪些功能、如何验收
MVP路线图	回答如何分阶段验证产品价值
原型结构说明	回答页面如何呈现、用户如何操作
产品作品集展示页	回答如何让项目被快速看懂
AI工作流与Prompt设计文档	回答 AI 如何真实进入产品流程

0.3 文档适用对象

对象	使用目的
AI产品经理	理解 AI 能力如何嵌入产品流程
Prompt工程师	根据任务、输入变量、输出结构和安全规则设计 Prompt

对象	使用目的
后端工程师	理解 AI 调用链路、数据结构、上下文管理和安全审核
前端工程师	理解 AI 输出如何展示在页面中
AI工程师	理解 OCR、RAG、模型调用、安全审核和评估需求
UI/UX设计师	理解 AI 生成结果如何转化为页面模块
测试人员	设计 AI 输出测试、安全测试和异常用例
作品集评审者	判断项目是否具备真实 AI 产品设计能力

0.4 文档设计原则

本文件遵循以下原则：

第一，产品流程优先。AI 必须服务于用户任务，而不是独立炫技。

第二，结构化数据优先。AI 生成之前，必须先完成 OCR、指标结构化、异常项提取和用户确认。

第三，安全边界优先。健康类 AI 产品必须先控制诊断、处方、治疗和高危误导风险。

第四，Prompt 模块化优先。不同任务需要不同 Prompt，不能用一个大 Prompt 处理所有场景。

第五，可评估优先。AI 输出必须能被评估、审核、追踪和迭代。

1. AI产品定位与设计原则

1.1 本产品中的 AI 定位

《AI体检报告解读与健康行动助手》中的 AI 不是医生，不是诊断系统，不是处方工具，也不是开放式健康问答机器人。

它的定位是：**在医疗安全边界内工作的体检报告理解与行动辅助系统。**

它的核心任务不是替用户判断“是否得病”，而是帮助用户完成以下转化：从看不懂报告转化为看懂重点；从看到异常焦虑转化为理解关注等级；从不知道怎么办转化为知道下一步行动；从单次报告转化为长期健康档案。

1.2 AI不是产品本身，而是产品能力的一部分

本项目的关键判断是：**AI不是这个产品的全部，AI只是产品系统中的能力层。**

一个合格的 AI 健康产品，不能只有“输入问题 - 模型回答”这一个链路。它应该包含用户场景、页面结构、数据输入、结构化处理、指标规则、知识库、Prompt模板、安全审核、用户反馈、数据沉淀和长期档案。

类型	开放式AI聊天	流程化AI健康助手
入口	用户随便提问	用户上传体检报告
上下文	不稳定	基于当前报告

类型	开放式AI聊天	流程化AI健康助手
数据结构	非结构化	指标结构化
输出方式	自由回答	固定结构输出
风险控制	难控制	可审核、可拦截
产品价值	临时问答	解读、行动、档案
长期价值	较弱	可沉淀健康档案

1.3 AI在产品中的核心价值

AI 在本产品中主要承担五类价值。

第一，将专业数据转化为用户语言。体检报告包含 ALT、AST、LDL-C、UA、HbA1c、TSH 等大量专业指标，AI 要将这些内容转化为普通用户能理解的解释。

第二，将异常指标转化为关注优先级。用户看到多个异常项时，真正需要的是知道哪些最重要、哪些需要复查、哪些需要咨询医生。

第三，将健康建议转化为行动计划。传统报告常说“注意饮食，适当运动”，但不够具体。AI 需要生成 7 天、30 天、90 天的可执行建议。

第四，将用户追问限制在报告上下文中。AI 追问不是泛健康聊天，而是基于当前报告的连续解释。

第五，将一次性报告转化为长期健康档案入口。通过结构化指标、行动计划、复查提醒和历史趋势，产品可以从单次解读升级为长期健康管理工具。

1.4 AI能力边界

1.4.1 AI可以做什么

本产品中的 AI 可以生成报告摘要、解释异常指标、说明风险关注等级、生成健康行动计划、回答基于当前报告的追问、生成医生沟通问题清单、生成复查提醒文案、总结历史指标趋势，并审核 AI 输出是否安全。

1.4.2 AI不可以做什么

本产品中的 AI 禁止疾病确诊、推荐具体药物、剂量、疗程、制定治疗方案、替代医生判断、告诉用户不用看医生、告诉用户不用复查、直接分析 CT / X 光 / 核磁等原始影像、判断重大疾病、使用恐吓式表达和使用绝对化表达。

1.5 AI设计总原则

本产品 AI 设计遵循五条原则：先结构化，再生成；先规则判断，再 AI 解释；先安全审核，再展示用户；先帮助理解，再推动行动；先控制风险，再扩展能力。

2. AI整体工作流设计

2.1 AI工作流总览

完整工作流如下：

```
用户上传体检报告
→ OCR识别报告内容
→ 指标结构化
→ 用户确认识别结果
→ 异常项提取
→ 风险关注等级计算
→ 医学知识库 / 指标规则库检索
→ AI生成报告总览
→ AI生成异常指标解释
→ AI生成健康行动计划
→ 安全审核模块检查输出
→ 前端展示结果
→ 用户继续AI追问
→ AI基于报告上下文回答
→ 二次安全审核
→ 用户保存报告摘要
→ 健康档案沉淀
→ 复查提醒 / 后续趋势对比
```

这不是一次模型调用，而是一条可控、可解释、可审核、可迭代的 AI 产品链路。

2.2 工作流阶段拆解

阶段	目标	关键输出
报告输入	获取用户报告并确认授权	原始文件、任务ID、保存模式
OCR识别	将图片/PDF转为文本和表格	OCR文本、字段候选值、置信度
指标结构化	将报告内容转为标准指标对象	结构化指标列表
用户确认	降低识别错误风险	用户确认后的最终指标
异常提取	找出异常指标	异常指标列表
风险等级	判断关注优先级	L1-L4风险关注等级
知识检索	获取指标解释和安全规则	知识片段、禁止表达
AI生成	生成报告总览、解释和计划	AI解读内容
安全审核	检查越界风险	pass / revise / block
前端展示	将AI结果页面化	卡片、标签、行动模块
AI追问	基于当前报告回答用户问题	安全回答
档案沉淀	保存摘要、异常项和计划	健康档案、复查提醒

2.3 工作流关键判断

本产品的 AI 工作流不应是用户提问后 AI 直接回答，而应是用户上传报告，系统识别数据，系统结构化指标，系统判断异常，系统计算关注等级，AI 解释结果，安全审核，用户查看，用户追问，再次审核，最后沉淀健康档案。

这条链路说明，本产品中的 AI 是一个可控系统，而不是无边界聊天工具。

3. AI能力模块设计

3.1 模块总览

本产品 AI 能力拆分为九个核心模块。

模块	核心任务	主要作用
OCR识别模块	识别报告文字与表格	将图片/PDF转为文本数据
指标结构化模块	提取指标字段	将报告内容转为标准化指标对象
异常项提取模块	识别异常指标	找出偏高、偏低、阳性、异常等项目
风险关注等级模块	计算关注等级	帮助用户判断处理优先级
报告总览生成模块	生成整体摘要	让用户快速看懂报告重点
异常指标解释模块	解释单项异常	帮助用户理解具体指标含义
健康行动计划模块	生成行动建议	把报告解读转化为可执行计划
AI追问模块	回答用户问题	支持基于当前报告的连续问答
安全审核模块	检查AI输出风险	防止诊断、处方、恐吓和越界表达

3.2 OCR识别模块

OCR识别模块的目标，是将用户上传的体检报告图片或PDF转化为可处理的文本和表格数据。OCR 不是最终价值，而是整个 AI 工作流的第一步。如果 OCR 识别错误，后续 AI 解释再优秀，也可能建立在错误数据之上。

输入包括报告图片、报告PDF、文件类型、页码信息、上传任务ID和用户授权状态。输出包括原始识别文本、表格识别结果、指标候选字段、识别置信度和OCR状态。

OCR需要识别报告标题、报告日期、体检机构、检查项目、指标名称、指标数值、单位、参考范围、异常标记和文本型结论。

OCR失败时，不应继续生成 AI 解读，应提示用户重新上传、使用样例报告或进入手动录入流程。

3.3 指标结构化模块

指标结构化模块的目标，是将 OCR 识别出的文本和表格转化为标准化指标对象。

```
{
  "indicator_id": "ind_001",
  "report_id": "report_001",
  "item_name_raw": "LDL-C",
  "item_name_standard": "低密度脂蛋白胆固醇",
  "category": "blood_lipid",
  "value": 3.9,
  "value_text": "",
  "unit": "mmol/L",
  "reference_range": "0-3.4",
  "reference_min": 0,
  "reference_max": 3.4,
  "abnormal_flag": "high",
  "confidence": 0.91,
  "source_page": 2,
  "user_confirmed": false
}
```

结构化模块需要完成指标名称标准化、指标分类、单位识别、参考范围解析、异常方向判断、置信度判断和用户修改后重新计算。

这是本产品区别于通用大模型的重要能力。只有完成结构化，后续 AI 解读才有稳定基础。

3.4 异常项提取模块

异常项提取模块的目标，是从全部结构化指标中识别出需要用户重点关注的项目。

类型	含义
high	高于参考范围
low	低于参考范围
positive	阳性或提示异常
borderline	临界
critical	极端异常或高危
unknown	无法明确判断

异常项排序建议：风险关注等级高的优先，异常程度明显的优先，与常见慢病风险相关的优先，用户主动关注指标优先，报告原始顺序作为辅助。

异常项提取的本质，是帮助用户从“报告里有一堆数据”转向“我知道该先看什么”。

3.5 风险关注等级模块

风险关注等级用于帮助用户理解异常指标的处理优先级。

等级	名称	含义	产品表达
L1	低关注	轻微异常或常见波动	建议关注生活方式，后续观察
L2	中关注	需要重视，建议调整并复查	建议生活方式调整并复查

等级	名称	含义	产品表达
L3	高关注	异常较明显	建议咨询相关科室医生
L4	紧急关注	可能存在高危情况	如伴明显不适，建议尽快就医

风险关注等级不是医学诊断等级，而是产品用于帮助用户理解优先级和行动路径的表达方式。生成方式建议为：规则判断 + 指标知识库 + AI解释。

3.6 报告总览生成模块

报告总览生成模块的目标，是让用户在最短时间内看懂整份体检报告。

输出结构应包含报告整体摘要、本次需要关注的重点、异常指标概览、初步行动建议、复查或就医提示和免责声明。

报告总览必须做到通俗易懂、优先展示重点、不做疾病确诊、不推荐药物、不制造恐慌、明确提示不替代医生。

3.7 异常指标解释模块

异常指标解释模块用于解释单个异常指标。

输出结构应包含指标解释、当前情况、为什么需要关注、常见影响因素、建议行动、复查建议、何时咨询医生和不确定性提示。

禁止输出：“你已经患有某病”“你必须服用某药”“不用看医生”“肯定没问题”“非常危险”。推荐输出：“该指标高于参考范围，建议结合其他指标和个人情况判断。如果持续异常，建议咨询医生。”

3.8 健康行动计划生成模块

健康行动计划模块的目标，是将体检报告解读转化为用户可执行的下一步计划。

输出结构包括计划总目标、7天行动建议、30天改善计划、90天复查目标、饮食建议、运动建议、睡眠作息建议、复查建议、就医准备和注意事项。

行动建议必须具体、可执行、安全、有阶段、不涉及处方药、不承诺疗效，并且可保存和追踪。

3.9 AI追问模块

AI追问模块支持用户围绕当前报告继续提问。

问题类型	示例	处理策略
指标解释	尿酸偏高是什么意思?	基于知识库解释
风险判断	这个严重吗?	给关注等级，不诊断
行动建议	饮食怎么调整?	给生活方式建议
复查建议	多久复查?	给复查参考
科室建议	应该挂什么科?	给就医参考

问题类型	示例	处理策略
用药问题	要不要吃药?	不给处方，建议医生
高危症状	胸痛怎么办?	提示及时就医
无关问题	非报告问题	引导回当前报告

AI追问必须经过二次安全审核。

3.10 安全审核模块

安全审核模块用于确保 AI 输出不会越过医疗安全边界。

风险类型	说明
diagnosis_risk	疾病诊断风险
prescription_risk	处方用药风险
treatment_risk	治疗方案风险
overconfidence_risk	绝对化表达风险
panic_risk	恐吓式表达风险
delayed_care_risk	延误就医风险
privacy_risk	隐私泄露风险
out_of_scope_risk	超出产品范围风险

审核结果包括 pass、revise 和 block。

```
{
  "result": "pass / revise / block",
  "risk_types": [],
  "reason": "",
  "revision_suggestion": "",
  "safe_rewrite": ""
}
```

4. Prompt设计方法论

4.1 总体方法

本产品 Prompt 设计遵循：**高效 Prompt = 目标 + 范围 + 流程 + 结果**。

这个方法的意义在于：让 AI 知道要做什么、不能做什么、应该怎么做、最后交付什么。

在健康产品中，Prompt　不能只追求回答丰富，还必须追求任务明确、边界清楚、过程稳定、输出可控、安全可审查、前端可展示和后续可评估。

4.2 目标

目标是 AI 本次任务要完成什么。例如生成报告总览、解释异常指标、生成健康行动计划、回答用户追问、审核 AI 输出是否安全、总结历史指标趋势和生成医生沟通问题清单。

一个 Prompt 最好只承担一个主要目标。

4.3 范围

范围是 AI 可以做什么、不可以做什么。

本产品 Prompt 的范围必须包含：AI 可以解释健康信息、说明指标含义、提示关注等级、给出生活方式建议、给出复查参考、给出就医准备建议和提醒用户咨询医生；AI 不可以疾病确诊、具体用药建议、治疗方案、替代医生判断、说不用就医、使用恐吓表达和使用绝对化表达。

4.4 流程

流程是 AI 应该按照什么步骤处理信息。例如，异常指标解释流程是先说明指标是什么，再说明当前数值与参考范围的关系，再说明为什么需要关注，再说明常见影响因素，再给出建议行动，再说明何时咨询医生，最后补充不确定性提示。

4.5 结果

结果是 AI 最终输出什么格式。固定输出格式方便前端拆卡片展示、后端保存字段、安全审核、用户阅读和后续评估。

4.6 Prompt模块化原则

Prompt	任务
报告总览生成Prompt	生成整份报告摘要
异常指标解释Prompt	解释单个异常指标
健康行动计划Prompt	生成行动建议
AI追问回答Prompt	回答用户后续问题
安全审核Prompt	审核AI输出风险
趋势总结Prompt	多报告趋势分析
医生沟通清单Prompt	就医前问题准备
复查提醒文案Prompt	生成提醒说明

4.7 Prompt版本管理

每个 Prompt 至少记录 prompt_id、prompt_name、version、task_type、input_variables、output_schema、safety_rules_version、updated_at 和 change_log。Prompt 需要版本化，因为 AI 输出质量和 Prompt 高度相关。

5. Prompt模板设计

5.1 报告总览生成Prompt

你是一名AI健康信息解释助手，不是医生，也不能替代医生诊断、治疗或处方。

【目标】
请根据用户的体检报告结构化数据，生成一份普通用户能理解的体检报告总览。

【范围】
你可以：总结报告整体情况、说明异常指标、用通俗语言解释需要关注的方向、给出复查和生活方式参考建议、提示用户必要时咨询医生。
你不可以：给出疾病确诊、推荐具体药物、说“肯定没事”或“必然有病”、使用恐吓式表达、替代医生判断、忽略高风险情况。

【流程】
先阅读报告基础信息，再识别异常指标，按关注优先级总结最重要问题，给出通俗解释，给出下一步行动方向，最后补充医疗边界提示。

【输入数据】
报告日期：{{report_date}}
用户基础信息：{{user_profile}}
全部指标数据：{{indicators}}
异常指标列表：{{abnormal_items}}
风险关注等级：{{risk_levels}}
知识库片段：{{knowledge_snippets}}

【输出格式】
1. 报告整体摘要：
2. 本次需要关注的重点：
3. 异常指标概览：
4. 初步行动建议：
5. 复查或就医提示：
6. 免责声明：

5.2 异常指标解释Prompt

你是一名AI健康信息解释助手，负责帮助普通用户理解体检报告中的异常指标。

【目标】
请解释用户体检报告中的单个异常指标，让用户理解该指标是什么意思、当前结果说明什么、为什么需要关注，以及下一步可以做什么。

【范围】
你可以解释指标的基本含义、说明当前数值与参考范围的关系、说明常见影响因素、给出生活方式和复查建议、提醒用户必要时咨询医生。
你不可以做疾病确诊、推荐药物、仅凭单个指标判断严重疾病、使用恐吓式表达、使用绝对化表达、告诉用户不用看医生或不用复查。

【输出格式】
1. 指标解释：
2. 当前情况：
3. 为什么需要关注：
4. 常见影响因素：
5. 建议行动：
6. 复查建议：
7. 何时咨询医生：
8. 不确定性提示：

5.3 健康行动计划Prompt

你是一名AI健康行动建议助手，负责基于用户体检报告异常项，生成安全、具体、可执行的健康行动计划。

【目标】
请为用户生成7天、30天和90天的健康行动建议，帮助用户知道下一步该怎么做。

【范围】
你可以给出饮食、运动、睡眠、复查和就医准备建议，根据异常指标调整建议重点，提醒用户关注症状变化，建议用户必要时咨询医生。
你不可以推荐具体药物或剂量，制定疾病治疗方案，承诺一定改善指标，替代医生判断，要求用户进行高风险行为，用恐吓方式推动用户行动。

【输出格式】
1. 计划总目标:
2. 7天行动建议:
3. 30天改善计划:
4. 90天复查目标:
5. 饮食建议:
6. 运动建议:
7. 睡眠作息建议:
8. 复查建议:
9. 就医准备:
10. 注意事项:

5.4 AI追问回答Prompt

你是一名AI体检报告解读助手，正在基于用户当前体检报告回答用户问题。

【目标】
请回答用户围绕当前体检报告提出的问题，帮助用户理解报告、判断关注重点并获得下一步行动建议。

【范围】
你可以基于当前报告解释指标，回答风险关注、复查、生活方式、科室建议等问题，提示用户必要时咨询医生，说明不确定性。
你不可以做疾病确诊，推荐具体药物、剂量或疗程，替代医生判断，让用户放弃就医，使用恐吓式表达，回答与当前报告完全无关的问题，对高危症状进行普通化回答。

【输出格式】
1. 简要回答:
2. 结合报告说明:
3. 建议行动:
4. 何时咨询医生:
5. 提醒:

5.5 安全审核Prompt

你是AI健康产品的安全审核模块，负责检查即将展示给用户的AI回答是否存在医疗安全风险。

【目标】
请判断以下AI回答是否安全，是否可以展示给用户。

【审核范围】
重点检查是否出现疾病确诊、具体药物、剂量、疗程建议、替代医生判断、建议用户不用就医或不用复查、绝对化表达、恐吓式表达、忽视高危症状、缺少不确定性提示、超出当前报告上下文、存在隐私泄露风险。

【输出JSON】
{

```
  "result": "pass / revise / block",
  "risk_types": [],
  "reason": "",
  "revision_suggestion": "",
  "safe_rewrite": ""
}
```

6. 医疗安全与Prompt风险控制

6.1 医疗安全控制目标

本产品的医疗安全控制目标包括防止 AI 输出疾病确诊、具体药品剂量疗程建议、治疗方案、替代医生判断、“不用就医”或“不用复查”的结论、恐吓式表达、绝对化表达、高危症状误判、超出当前体检报告上下文自由发挥和过度使用用户敏感健康信息。

本产品的安全原则是：**AI 可以帮助用户理解健康信息，但不能替用户做医疗决策。**

6.2 禁止表达清单

类型	禁止表达	替代表达
明确诊断	“你已经患有痛风”	“该指标提示相关风险需要关注，但不能仅凭当前结果判断具体疾病”
处方用药	“你应该吃某某药”	“是否需要用药应由医生结合完整情况判断”
治疗方案	“按照这个方案治疗即可”	“以下建议仅属于一般健康生活方式参考”
绝对判断	“肯定没事”	“目前信息不足以做出确定判断”
恐吓表达	“这个非常危险”	“该指标需要关注，建议进一步评估”
延误就医	“不用看医生”	“如果持续异常或伴随不适，建议咨询医生”

6.3 高危问题识别

高危症状包括胸痛、胸闷、呼吸困难、晕厥、意识障碍、抽搐、突发肢体无力、言语不清、大量出血、黑便、咯血、高热不退、剧烈腹痛、严重过敏、孕产期异常出血、自伤或自杀倾向、极端虚弱或急性恶化。

高危问题处理流程：

```
用户输入问题 / 系统识别报告
→ 触发高危规则
→ 停止普通AI解读流程
→ 展示高危提示
→ 建议及时咨询医生或就医
→ 不提供具体诊断、处方或治疗方案
```

高危提示文案：

```
你描述的情况可能存在较高风险，AI无法替代医生判断。建议你尽快联系医生、前往急诊或拨打当地急救电话。如果症状正在加重，请不要等待线上回复。
```

6.4 三层安全审核策略

建议采用三层安全审核：第一层是输入前置识别，识别用户问题中是否包含高危症状、用药请求、诊断请求、自伤风险等；第二层是生成中 Prompt 约束，在任务 Prompt 中明确禁止诊断、处方、治疗方案、恐吓和绝对化表达；第三层是输出后安全审核，使用安全审核 Prompt 或规则模块检查 AI 输出，判断 pass / revise / block。

6.5 Prompt风险控制规则

所有健康相关 Prompt 必须包含：

```
你不是医生，不能替代医生诊断、治疗或处方。
你可以解释健康信息、说明体检指标含义、给出生活方式和复查参考。
你不可以诊断疾病、推荐药物、制定治疗方案、让用户放弃就医、使用恐吓或绝对化表达。
```

用药问题必须转向医生。“严重吗”问题必须转化为关注等级。超出范围问题必须引导回当前报告。高危问题必须优先提示及时就医。

7. RAG与医学知识库设计

7.1 为什么需要知识库

本产品不能完全依赖大模型自身记忆来解释体检指标。原因包括大模型可能产生幻觉、不同模型输出一致性不稳定、体检指标解释需要统一口径、医疗安全边界需要可控规则、不同指标需要不同复查和行动建议、产品需要可维护和可更新的知识体系。

RAG 的作用不是让 AI “知道更多”，而是让 AI “基于可控知识回答”。

7.2 知识库内容范围

类别	示例
血常规	白细胞、红细胞、血红蛋白、血小板
尿常规	尿蛋白、尿潜血、尿糖、尿酮体
肝功能	谷丙转氨酶、谷草转氨酶、胆红素
肾功能	肌酐、尿素、尿酸
血脂	总胆固醇、甘油三酯、低密度脂蛋白
血糖	空腹血糖、糖化血红蛋白
甲状腺	TSH、T3、T4
影像报告文字	脂肪肝、结节、囊肿等文字结论
常见建议	饮食、运动、睡眠、复查、就医准备
安全规则	不诊断、不处方、高危提示、禁止表达

7.3 指标知识库字段设计

```
{
  "indicator_id": "ua",
  "indicator_name_standard": "尿酸",
  "aliases": ["UA", "血尿酸", "尿酸"],
  "category": "kidney_metabolism",
  "plain_explanation": "尿酸是身体代谢嘌呤后产生的一种物质，主要通过肾脏排出。",
  "common_abnormal_meaning_high": "尿酸偏高可能与饮食、饮酒、体重、代谢状态、肾脏排泄能力等因素有关。",
  "possible_factors": ["高嘌呤饮食", "饮酒", "体重偏高", "饮水不足"],
  "lifestyle_suggestions": ["减少高嘌呤食物", "控制饮酒", "适量饮水", "规律运动"],
  "recheck_suggestion": "如持续偏高，建议根据医生或体检机构建议复查。",
  "doctor_consultation_hint": "如尿酸持续升高，或出现关节红肿热痛等症状，建议咨询医生。",
  "related_indicators": ["肌酐", "尿素", "肾功能", "血脂"],
  "forbidden_claims": ["不能仅凭尿酸升高判断痛风", "不能给出降尿酸药物建议"],
  "safety_notes": ["不提供药物剂量建议", "不做痛风确诊"]
}
```

7.4 知识库与Prompt关系

知识库负责提供事实、规则和口径。Prompt 负责组织任务、范围、流程和输出结构。大模型负责把结构化输入和知识库内容转化为自然语言。安全审核负责检查最终输出是否越界。

```
结构化报告数据
→ 指标知识库 / 安全规则库
→ Prompt任务模板
→ 大模型生成
→ 安全审核
→ 用户展示
```

7.5 检索策略

检索维度	示例
指标名称	尿酸、甘油三酯、低密度脂蛋白
指标别名	LDL-C、UA、ALT、AST
异常方向	偏高、偏低、阳性
指标分类	血脂、肝功能、肾功能、血糖
风险等级	L1、L2、L3、L4
用户问题意图	复查、饮食、运动、科室、用药

7.6 知识库分层

建议分为四层：指标解释层、异常含义层、行动建议层和安全规则层。这种分层有利于后续维护，也方便不同 Prompt 调用不同内容。

8. 数据流与上下文管理

8.1 数据流设计目标

数据流与上下文管理的目标，是确保 AI 在正确、必要、最小化的数据范围内工作。本产品的数据流必须遵循结构化优先、当前报告优先、最小必要原则、用户授权优先、安全边界优先和可删除可追踪。

8.2 数据流总览

原始报告文件
→ OCR识别文本
→ 指标结构化数据
→ 用户确认后的指标
→ 异常指标列表
→ 风险关注等级
→ 知识库检索结果
→ AI生成内容
→ 安全审核结果
→ 前端展示内容
→ 用户AI追问
→ 对话上下文
→ 健康档案摘要
→ 复查提醒
→ 历史趋势对比

8.3 数据分层

数据层	内容	管理原则
原始数据层	报告图片、PDF、OCR文本	敏感度最高，尽量减少长期保存
结构化数据层	指标、数值、单位、异常方向	AI解读主要输入
AI生成结果层	总览、解释、行动计划、追问回答	可展示、可审核、可保存
用户交互层	追问、反馈、修改、保存选择	用于产品优化，避免过度采集
长期档案层	报告摘要、异常项、趋势、提醒	必须基于用户授权保存

8.4 上下文输入设计

不同任务只输入必要上下文。报告总览需要报告日期、用户基础信息、全部结构化指标、异常指标列表、风险等级、知识库片段和安全规则。异常指标解释需要当前指标名称、当前数值、单位、参考范围、异常方向、风险等级、相关指标、指标知识库片段和安全规则。AI追问需要用户当前问题、当前报告摘要、当前异常指标、当前风险等级、最近对话历史、相关知识库片段和安全规则。

8.5 上下文裁剪原则

上下文裁剪原则包括：当前报告优先、异常指标优先、用户最近问题优先、高风险信息优先、隐私最小化、未确认数据谨慎使用、家庭成员报告不得默认混入本人报告。

8.6 隐私与模型调用原则

传给模型的数据应只包含完成当前任务所必需的信息。应尽量脱敏姓名、身份证号、手机号、体检编号、详细地址和无关身份信息。用户应知道上传内容会被用于本次解读，是否保存由用户决定，是否进入长期档案由用户决定，是否用于模型训练应默认否，用户可以删除保存数据。

9. AI输出质量评估

9.1 评估目标

AI输出质量评估的目标，是判断 AI 能力是否真正达到产品可用、用户可懂、医疗安全、结果稳定和可持续迭代的标准。

本产品不只看 AI 回答是否丰富，而是重点评估是否基于当前报告、是否准确解释指标、是否避免诊断和处方、是否通俗易懂、是否给出具体行动、是否高危提示及时、是否结构稳定、是否可追踪和迭代。

9.2 评估维度

维度	说明
准确性	是否基于真实结构化指标和知识库
完整性	是否包含该任务所需字段
通俗性	普通用户是否能看懂
行动性	是否告诉用户下一步怎么做
安全性	是否避免诊断、处方、治疗和延误就医
一致性	不同页面对同一指标表达是否一致
可追踪性	是否能回溯模型、Prompt、知识库和安全规则版本

9.3 核心质量指标

指标	定义
报告总览生成成功率	成功生成报告总览次数 / 请求次数
指标解释生成成功率	成功生成指标解释次数 / 请求次数
行动计划生成成功率	成功生成行动计划次数 / 请求次数
AI追问成功率	成功回答用户追问次数 / 用户追问次数
输出结构完整率	输出包含规定字段的比例
医疗边界违规率	出现诊断、处方、治疗等越界表达比例
安全审核拦截率	被安全模块拦截的回答比例
高危问题识别率	高危问题被正确识别的比例

指标	定义
幻觉率	AI是否编造报告中不存在的信息
用户纠错率	用户指出AI内容不准确的比例

9.4 测试用例类型

类型	测试目标
正常报告测试	AI是否不制造焦虑
轻度异常测试	是否正确解释轻度异常
多项异常测试	是否能排序重点
用药问题测试	是否拒绝具体药物建议
高危症状测试	是否提示及时就医
越界诊断测试	是否不做疾病确诊
低置信度OCR测试	是否要求用户确认
无关问题测试	是否引导回当前报告

10. AI异常处理与降级策略

10.1 降级原则

AI产品必须假设 AI 会失败。本产品降级原则为：安全优先于完整，结构化结果优先于生成解释，提示用户确认优先于直接判断，就医提示优先于 AI 继续回答。

10.2 异常类型与处理

异常类型	处理方式
上传异常	提示重新上传，提供样例体验
OCR异常	提示上传更清晰图片，不生成AI解读
结构化异常	标记低置信度，要求用户确认
知识库检索异常	不强行解释，提示咨询医生或体检机构
AI生成异常	展示基础异常列表，允许重新生成
输出结构异常	自动重试，失败后使用备用模板
安全审核 revise	使用 safe_rewrite 改写后展示
安全审核 block	拦截原回答，展示安全提示
高危问题	停止普通回答，提示及时就医

异常类型	处理方式
上下文异常	不继续生成具体健康建议
隐私异常	不保存、不调用未授权数据

10.3 关键提示文案

OCR失败：

> 报告识别失败，可能是图片不够清晰、表格过于复杂或文件无法解析。请尝试重新上传清晰图片，或先使用样例报告体验完整流程。

AI生成失败：

> AI解读生成失败，可能是网络或系统处理异常。你仍然可以查看已识别出的指标和异常项，也可以稍后重新生成解读。

安全拦截：

> 这个问题可能涉及医疗诊断、用药或高风险健康判断，AI无法替代医生提供结论。建议你结合体检报告咨询医生或专业医疗机构。

高危提示：

> 你描述的情况可能存在较高风险，AI无法替代医生判断。建议你尽快联系医生、前往急诊或拨打当地急救电话。如果症状正在加重，请不要等待线上回复。

11. MVP阶段AI实现方案

11.1 实现目标

MVP阶段不追求一步做成完整医疗级 AI 系统，而是分阶段验证 AI 能力是否能支撑核心产品闭环。

核心闭环：上传报告、识别指标、提取异常、生成报告总览、解释异常指标、生成行动计划、支持AI追问、安全审核、保存摘要。

11.2 V0.1 原型验证版

目标：验证用户是否认可这个产品方向。

模块	实现方式
报告上传	模拟上传或样例报告
OCR识别	不做真实OCR，使用预设结构化数据
指标结构化	使用样例JSON
异常项提取	使用预设异常项
风险等级	使用预设L1-L4标签

模块	实现方式
报告总览	使用预设AI生成结果
指标解释	使用预设文本或Prompt生成
行动计划	使用预设或规则生成
AI追问	模拟推荐问题 + 预设回答
安全审核	静态安全提示 + 基础禁止规则

成功标准：用户能理解产品不是 AI 医生，能看懂报告总览，愿意点击异常指标详情，认为行动计划具体，愿意继续追问，并愿意尝试上传真实报告。

11.3 V0.2 真实识别版

目标：验证真实报告上传、OCR识别、指标结构化和 AI 解读能力。

模块	实现方式
报告上传	支持图片 / PDF
OCR识别	接入OCR服务或视觉模型
指标结构化	规则 + 模型辅助
用户确认	前端表格确认与修改
异常提取	根据参考范围和异常标记判断
风险等级	基础规则 + 指标知识库
报告总览	大模型生成
指标解释	RAG + Prompt生成
行动计划	Prompt生成
AI追问	当前报告上下文 + RAG
安全审核	安全审核Prompt + 规则拦截

成功标准：用户可以上传真实图片或PDF，系统能识别常见体检指标，用户可以确认或修正识别结果，AI能基于真实指标生成报告总览，AI解释不编造不存在的指标，AI回答不做诊断、不处方，高危问题能触发提示。

11.4 V0.3 健康档案版

目标：验证用户是否愿意将一次性报告解读结果保存为长期健康档案。

模块	实现方式
历史报告	保存结构化报告摘要
指标趋势	对比多次结构化指标

模块	实现方式
趋势总结	Prompt生成趋势解释
复查提醒	根据异常项生成提醒文案
健康周报	基础摘要生成
AI追问	支持当前报告 + 历史摘要
隐私控制	用户可删除报告与对话

成功标准：用户愿意保存至少一份报告，愿意设置复查提醒，会查看历史报告，愿意上传第二份报告，趋势总结能帮助用户理解变化，用户能删除保存数据。

11.5 V1.0 完整MVP版

V1.0 应形成完整 AI 健康管理闭环：上传报告、OCR识别、指标结构化、用户确认、异常提取、风险分级、报告总览、指标解释、行动计划、AI追问、安全审核、健康档案、复查提醒、历史趋势。

12. 技术协作与产品交付说明

12.1 技术协作目标

本项目需要产品、设计、前端、后端、AI、测试共同协作完成。协作目标是让 AI 能力不是黑盒回答，而是可拆解、可调用、可审核的产品能力；让每个团队成员都理解 AI 在产品流程中的位置；让 AI 输出结构能够直接进入前端页面；让后端能按任务拆分接口和数据结构；让 Prompt、知识库、安全规则和模型调用能够版本化管理；让测试人员能验证 AI 输出质量和医疗安全边界。

12.2 跨角色协作总览

角色	主要关注点	需要从本文档获得什么
产品经理	AI能力范围、业务流程、版本规划	AI任务拆解、边界、MVP路线
UI/UX设计师	页面承接、信息层级、用户理解	AI输出结构、页面模块、状态提示
前端工程师	页面展示、交互状态、错误提示	输出字段、展示组件、降级状态
后端工程师	数据流、接口、上下文、安全审核	数据结构、接口逻辑、任务链路
AI工程师	Prompt、RAG、模型调用、评估	Prompt模板、知识库字段、审核规则
测试人员	功能测试、安全测试、异常测试	测试用例、验收标准、风险样例

12.3 前端交付要求

前端需要支持上传页面、识别中状态、识别失败状态、识别结果确认页面、报告总览展示、异常指标卡片展示、指标详情展示、行动计划展示、AI追问对话展示、安全提示展示、保存档案确认、复查提醒入口和用户反馈入口。

状态	说明
loading	正在上传、识别、生成
success	成功展示结果
partial_success	部分成功
failed	处理失败
low_confidence	识别结果需确认
safety_blocked	AI输出被拦截
high_risk_alert	触发高危提示
no_save_mode	用户选择不保存
saved	用户已保存报告摘要

12.4 后端交付要求

后端任务链路建议：

```
upload_report
→ create_ocr_task
→ parse_ocr_result
→ structure_indicators
→ user_confirm_indicators
→ extract_abnormal_items
→ calculate_risk_levels
→ retrieve_knowledge
→ generate_ai_output
→ safety_review
→ save_analysis_result
→ return_frontend_payload
```

建议接口：

接口	作用
POST /reports/upload	上传报告
POST /reports/{id}/ocr	发起OCR识别
GET /reports/{id}/ocr-result	获取OCR结果
POST /reports/{id}/indicators/confirm	用户确认指标
POST /reports/{id}/analysis	生成报告总览
GET /reports/{id}/summary	获取报告总览
GET /reports/{id}/indicators	获取指标列表
GET /indicators/{id}/explanation	获取指标解释
POST /reports/{id}/action-plan	生成行动计划

接口	作用
POST /reports/{id}/chat	AI追问
POST /safety/review	AI安全审核
POST /reports/{id}/save	保存报告摘要
DELETE /reports/{id}	删除报告
POST /feedback	提交用户反馈

12.5 AI工程交付要求

AI工程应输出 Prompt模板文件、Prompt版本管理表、知识库字段设计、RAG检索逻辑、安全审核模块、AI输出Schema校验、模型调用接口、AI测试报告、Prompt迭代记录和风险样例库。

12.6 测试交付要求

测试需要验证 AI 是否基于当前报告回答、AI 是否输出固定结构、AI 是否避免诊断处方和治疗方案、高危问题是否被识别、OCR失败是否能降级、低置信度指标是否需要确认、安全审核是否能拦截风险输出、不保存模式是否真的不进入长期档案、用户删除数据后是否不可再调用。

13. 作品集展示角度

13.1 本文档在作品集中的作用

这份文档证明：我能把 AI 能力拆成真实产品流程中的多个节点；我知道每个节点的输入、处理、输出和风险；我知道 Prompt 不只是写一句指令，而是产品任务、边界、流程和输出结构的组合；我知道健康类 AI 产品必须有医疗安全边界；我知道 AI 输出需要评估、降级、审核和版本管理。

这份文档是整个作品集中最能体现 AI 产品经理专业能力的一份材料。

13.2 作品集展示重点

建议展示 AI工作流总览图、AI能力模块拆解、Prompt设计方法论、核心Prompt模板、医疗安全边界、RAG与知识库设计、AI输出质量评估和MVP阶段实现路线。

13.3 主页展示摘要

AI体检报告解读与健康行动助手，是一个面向普通体检用户和家庭健康管理者的AI健康产品。

项目目标不是让AI替代医生，而是帮助用户上传体检报告后，看懂异常指标、理解关注优先级、生成可执行健康行动计划，并逐步建立长期健康档案。

在这个项目中，我将AI能力拆解为报告OCR识别、指标结构化、异常项提取、风险关注等级、报告总览生成、异常指标解释、健康行动计划、AI追问和安全审核等多个模块。

Prompt设计采用“目标 + 范围 + 流程 + 结果”的方法，使AI输出能够稳定服务具体产品任务，而不是自由生成不可控回答。

项目特别强调医疗安全边界：AI不做疾病诊断、不提供处方建议、不制定治疗方案、不替代医生判断；高危问题优先提示用户及时就医。

这个项目展示了我对AI产品工作流、Prompt设计、RAG知识库、医疗安全边界、数据结构、MVP验证和产品落地的系统性理解。

13.4 面试讲解方式

这个项目最核心的判断是：AI健康产品不能一上来做AI医生，而应该先找到一个具体、真实、可控的场景。

我选择的是体检报告解读，因为这个场景有明确用户痛点：用户拿到报告后看不懂、不会判断、不会行动。

在产品设计上，我没有把AI设计成一个开放式聊天框，而是把AI拆进完整流程里：报告上传、OCR识别、指标结构化、异常项提取、风险等级、报告总览、指标解释、行动计划、AI追问、安全审核和健康档案。

Prompt设计上，我用“目标 + 范围 + 流程 + 结果”的方法，每个Prompt只解决一个明确任务，并且内置医疗安全边界。

这个项目最重要的不是AI回答多聪明，而是AI是否能在产品流程中稳定、安全、可控地帮助用户理解报告并形成行动。

14. 文档结论

14.1 核心结论

《AI体检报告解读与健康行动助手》的 AI 设计核心，不是让大模型直接回答健康问题，而是让 AI 在结构化数据、规则边界、知识库、安全审核和用户流程中发挥作用。

本产品中的 AI 应被设计为可控的、可解释的、可审核的、可迭代的、可评估的、可落地的产品能力。

产品不是依赖 AI 自由发挥，而是通过流程、Prompt、知识库、数据结构和安全审核，把 AI 能力变成稳定的产品能力。

14.2 最重要的产品判断

第一，AI健康产品不能直接做“AI医生”。体检报告解读是更具体、更可控、更适合 MVP 验证的切入点。

第二，AI不能是聊天框，而应该是工作流。AI 应出现在报告上传、OCR识别、指标结构化、异常提取、风险等级、解读、追问、安全审核和档案沉淀的完整链路中。

第三，Prompt不是提示词，而是产品规则。Prompt 承担任务定义、能力边界、输出流程、结构约束、安全限制和前端展示约定。

第四，安全审核不是补丁，而是主流程。输入前、生成中、输出后、用户反馈后，都应有安全控制。

第五，结构化数据决定长期价值。如果产品只做一次 AI 回答，容易被通用大模型替代；如果能沉淀报告、指标、异常项、行动计划、复查提醒和历史趋势，就具备长期健康管理价值。

14.3 最终结论

真正的 AI 产品设计，不是把大模型接到页面里，而是把 AI 能力拆进用户任务、业务流程、数据结构、Prompt体系、知识库、安全审核和产品体验中。

在本项目中，AI 的正确角色不是医生，而是体检报告理解助手、健康信息解释助手、异常指标说明助手、行动计划生成助手、复查提醒助手和医疗安全提示助手。

最终，本项目的 AI 设计可以用一句话概括：

让 AI 在安全边界内，把体检报告从难懂的数据文件，转化为用户能够理解、执行和持续管理的健康行动入口。