ICS 35.240.80

CCS C07

团　　体　　标　　准

T/NAHIEM XXX-2026

基于大模型的医院智能平台建设与语音技术应用规范

Construction of a Hospital Intelligent Platform Based on Large Models and Standards for Voice Technology Application

2026-XX-XX 发布　　2026-XX-XX 实施

全国卫生产业企业管理协会　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。

本文件由全国卫生产业企业管理协会医院质量管理与信息化建设分会提出。

本文件由全国卫生产业企业管理协会归口。

本文件起草单位：华中科技大学同济医学院护理学院、华中科技大学土木与水利工程学院、北京市建筑设计研究院股份有限公司、武汉市第四医院、湖北省肿瘤医院、温州医科大学护理学院、华中科技大学同济医学院附属协和医院、华中科技大学同济医学院附属同济医院、湖北中医药大学护理学院、武汉大学中南医院、中山大学护理学院、全国卫生产业企业管理协会医院质量管理与信息化建设分会、深圳市罗湖区人民医院。

本文件主要起草人：李节、王芙蓉、夏平、郑琪、周迎、付文宁、李素云、张丽华、王玫、李菊芳、乔桂圆、白雪、袁金蓉、潘丽、熊晓菊、熊甜、徐嘉琦、田翀、张可可、陶佳鑫、肖辉、夏薇、刘姗、刘晓娟、张悦、杨柳清、赵浩丞、李苗。

引 言

本文件的制定旨在规范基于大模型的医院智能平台与语音技术的研发、建设与应用，提升医疗服务的智能化水平与数据安全治理能力。本标准围绕平台架构、数据管理、语音技术、功能要求、质量控制、临床责任等方面提出系统性要求，强调以患者为中心、安全可控、人机协同的基本原则，旨在推动人工智能技术在医疗领域的健康、合规与可持续发展。

基于大模型的医院智能平台建设与语音技术应用标准

1 范围

本文件规定了基于大模型的医院智能平台与语音技术的术语、架构、数据管理、功能要求、技术标准、质量控制与风险管理等方面的系统要求，提供了涵盖平台建设、语音技术应用、数据标注治理及临床责任划分的具体实施要求。

本文件适用于各级各类医疗机构开展智能平台建设、语音技术应用及相关管理与评估工作。

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。

DB34/T 4011-2021 《智慧医院建设指南》

DB34/T 4659-2024 《医院智慧安防建设指南》

DB34/T 4515-2023 《智慧医院评价指南》

GB/T 42018-2022 《信息技术人工智能平台计算资源规范》

GB/T 43782-2024 《人工智能—机器学习系统技术要求》

GB/T 44089-2024 《信息技术—全双工语音交互系统通用技术要求》

GB/T 35273-2020 《信息安全技术 个人信息安全规范》

GB/T 39725-2020 《信息安全技术 健康医疗数据安全指南》

YY/T 1833.3-2022 《人工智能医疗器械 质量要求和评价 第3部分：数据标注通用要求》

3 术语和定义

下列术语和定义适用于本文件。

3.1 基本术语

3.1.1

大模型　Large Model

大模型指基于深度学习架构、参数量巨大（通常达数十亿以上）、在海量多源数据上训练而成，能够通过预训练适应多种下游任务，并表现出涌现能力和强泛化性的人工智能模型。在本标准中，指针对医疗健康领域的数据和任务特点进行预训练或优化、参数量巨大、能够处理医学自然语言并支持临床辅助决策等智能应用的人工智能模型。

3.1.2

医院智能平台　Intelligent Hospital Platform

医院智能平台是指利用人工智能、大数据、云计算等技术，集成医院各类信息系统，实现医院管

理、诊疗服务、就诊服务等多个方面的智能化，提高医疗服务质量和效率。

3.1.3

语音技术　Speech Technology

语音技术包括语音识别(Automatic Speech Recognition, ASR)和语音合成(Text to Speech, TTS)，能够实现语音到文本的转换以及文本到语音的转换。在医院智能平台中，语音技术可以用于接诊人群信息录入、智能导诊、挂号系统管理、人力资源管理、检查结果审阅、危急值管理、院感管理以及满意度测评等场景。

3.2 相关术语

3.2.1

知识库　Knowledge Base

知识库是存储、管理和检索知识的信息库，它可以包含医学知识、临床指南、药物信息等。在医院智能平台中，知识库用于支持大模型提供准确的医疗建议和决策支持。

3.2.2

人工智能　Artificial Intelligence, AI

是利用数字计算机或由数字计算机控制的机器来模拟、延伸和扩展人类智能的理论、方法、技术及应用系统，如视觉识别、语言理解和决策。

3.2.3

机器学习　Machine Learning

人工智能的一个分支，是一种通过算法和模型使计算机从数据中自动学习并进行预测或决策的技术。

3.2.4

自然语言处理　Natural Language Processing

自然语言处理是人工智能和语言学领域的一个分支，旨在使计算机能够理解、解释和生成人类语言。在医疗智能平台中，NLP 技术用于解析医疗文档、患者咨询等自然语言文本。

3.2.5

语音识别　Speech Recognition

将人类的语音转换成计算机可理解的文本的技术。

3.2.6

语音合成　Text to Speech

将文本转换成类似人类的语音的技术。

3.2.7

智能语音交互　Intelligent Voice Interaction

利用语音识别和语音合成技术，实现人与计算机系统的自然语言交流。

3.2.8

数据安全　Data Security

保护数据不被盗窃、破坏或丢失的技术和过程。

3.3 数据标注相关术语

3.3.1

数据标注　Data Annotation

指通过人工、半自动或自动化的方式，对原始数据（如文本、图像、音频、视频）添加结构化标签、注释或元数据的过程。

3.3.2

标注角色　Annotation Role

指在数据标注工作流程中，承担不同职责与任务的参与者或岗位。建立清晰的角色体系是确保标注质量和效率的关键。

3.3.3

标注一致性　Annotation Consistency

指在同一个标注项目中,不同标注员之间或同一标注员在不同时间对相同或同类数据进行标注时，其标注结果保持统一和稳定的程度。

3.3.4

标注质量控制　Annotation Quality Control

指为确保数据标注结果满足预定义的质量标准与规范，而在标注全生命周期（包括标注前、标注中、标注后）实施的一系列计划性、系统性的管理活动和技术措施。

4 智能平台架构

4.1 硬件架构

医院智能平台的硬件架构通常包括高性能服务器、存储设备、网络设备以及前端交互设备。服务器负责处理大量的数据分析和模型运算，存储设备用于保存医疗数据和系统日志，网络设备保证数据的高速传输和安全性，而前端交互设备如自助服务机、智能导诊屏等直接与患者或医务人员交互。

4.2 软件架构

软件架构是医院智能平台的核心，涉及到操作系统、数据库管理系统、中间件以及应用程序。

4.2.1 操作系统：通常选择稳定性和安全性高的 Linux 或 Unix 系统。

4.2.2 数据库系统：使用关系型数据库如 MySQL 或 PostgreSQL 来存储结构化数据，非关系型数据库如 MongoDB 用于存储非结构化数据。

4.2.3 中间件：包括应用服务器、消息队列、缓存服务等，用于系统组件之间的通信和数据交换。

4.2.4 应用程序：开发基于大模型的智能应用，如语音识别、自然语言处理、图像识别等。

4.3 网络架构

4.3.1 内部网络：采用私有网络，确保医疗数据的安全传输。

4.3.2 外部网络：通过 VPN 或 API 网关与外部系统进行安全的数据交换。

4.3.3 云服务：部分计算和存储任务可以部署在云端，利用云计算的弹性和可扩展性。

5 数据管理

5.1 数据收集

5.1.1 数据来源与类型：

数据收集是医院智能平台建设的首要步骤，需要确立明确的数据来源与类型标准。数据来源应涵盖就诊人群医疗记录、诊疗过程、医疗设备数据、医院运营数据等多个方面。数据类型应包括但不限于结构化数据如电子病历、实验室结果，以及非结构化数据如医学影像、语音记录等。

a) 就诊人群医疗记录：确保收集就诊人群的基本信息、病史、药物使用记录等；

b) 诊疗过程数据：包括医生诊断记录、治疗计划、手术过程等关键信息；

c) 医疗设备数据：涉及医疗设备的状态监控、使用频率、维护记录等；

d) 医院运营数据：如就诊人群流量、病房使用情况、财务数据等。

5.1.2 数据质量与完整性

数据质量与完整性是确保医院智能平台有效运行的关键。应制定严格的数据质量控制流程，确保数据的准确性、一致性、及时性和可追溯性。

a) 准确性：通过数据校验机制确保收集的数据反映真实情况，减少输入错误；

b) 一致性：保证数据格式和标准在不同数据源和数据集中保持一致；

c) 及时性：确立数据更新频率，确保数据的时效性，满足临床决策需求；

d) 可追溯性：记录数据的来源、修改历史和访问记录，以支持数据审计和问题追踪。

此外，数据的收集应遵循相关法律法规，保护就诊人群隐私，如遵循《中华人民共和国个人信息保护法》等相关条例，对敏感数据进行脱敏处理，确保数据安全。

5.2 数据存储标准

5.2.1 数据存储安全

在基于大模型的医院智能平台建设中，数据存储安全是至关重要的一环。以下是数据存储安全应遵循的标准：

a) 数据加密：所有存储的数据必须进行加密处理，以防止未授权访问和数据泄露。应使用行业标准的加密算法，如 AES256；

b) 数据备份：定期对数据进行备份，并确保备份数据的安全性与可恢复性。备份应存储在安全的位置，最好是异地存储；

c) 数据完整性：采用校验和或哈希算法确保数据在存储和传输过程中的完整性，防止数据被篡改；

d) 物理安全：数据中心应具备严格的物理安全措施，包括但不限于访问控制、监控系统和环境控制。

5.2.2 数据访问控制

数据访问控制是保护数据不被未授权访问的另一重要方面。以下是数据访问控制应遵循的标准：

a) 身份验证：所有访问数据的用户必须通过强身份验证机制，如多因素认证；
b) 权限控制：根据用户的角色和职责，实施最小权限原则，确保用户只能访问其工作所必需的数据；
c) 访问审计：记录和监控所有数据访问活动，以便于事后审计和在发生安全事件时追踪问题源头；
d) 数据脱敏：对于需要在不安全或公共环境中访问的数据，应进行脱敏处理，以保护就诊人群隐私和敏感信息；
e) 安全协议：确保所有数据传输都通过安全协议，如 HTTPS 或 SSL/TLS，以防止数据在传输过程中被截获。

5.3 数据处理标准

5.3.1 数据处理流程

在构建基于大模型的医院智能平台时，数据处理流程是确保数据质量和安全性的关键。以下是数据处理流程的标准制定：

a) 数据收集：必须确保数据来源的合法性与合规性，遵循就诊人群隐私保护法规，如 HIPAA 或 GDPR。收集的数据应包括但不限于医疗记录、诊疗信息、就诊人群反馈等；
b) 数据存储：采用加密技术确保数据存储安全，设立访问控制机制，确保只有授权人员才能访问数据。同时，应定期备份数据以防数据丢失；
c) 数据清洗：对收集到的数据进行预处理，包括去除噪声、填补缺失值、格式统一等，以提高数据质量，为后续的分析和模型训练打下良好基础；
d) 数据整合：将不同来源和类型的数据进行整合，建立统一的数据仓库，便于数据的统一管理和快速检索；
e) 数据隐私保护：在数据收集、存储和处理的每个环节都应实施隐私保护措施，如匿名化处理、数据加密、访问审计等。

5.3.2 数据分析与应用

数据分析与应用是发挥大数据价值、提升医疗服务质量的重要环节。以下是数据分析与应用的标准制定：

a) 数据分析方法：采用先进的统计学方法和机器学习算法对数据进行深入分析；
b) 数据可视化：通过图表、图形等可视化手段直观展示数据分析结果；
c) 数据驱动决策：将数据分析结果应用于临床决策支持系统；
d) 数据安全与伦理：在数据分析与应用过程中，持续关注数据安全与伦理问题；
e) 数据反馈机制：建立数据反馈机制，将数据分析结果和应用效果反馈给数据收集与处理环节，不断优化数据处理流程和分析方法。

5.4 数据保护标准

5.4.1 隐私保护措施：涉及流程包括

a） 数据收集：必须遵循最小化原则，只收集实现服务所必需的数据，且在收集前需获得就诊人群的明确同意；

b） 数据存储：采用加密存储技术，确保数据在静态状态下的安全，防止未授权访问和篡改；

c） 数据访问控制：实施基于角色的访问控制策略，确保只有授权人员才能访问敏感数据，并对访问行为进行审计；

d） 数据脱敏处理：在数据展示、分析等操作中，对个人信息进行脱敏处理，避免泄露就诊人群身份；

e） 法律遵从性：遵循《中华人民共和国个人信息保护法》等相关法律法规，确保隐私保护措施的合法性。

5.4.2 数据泄露应对

数据泄露是医院智能平台面临的重大风险，需要制定以下应对措施：

a） 风险评估：定期进行数据安全风险评估，识别潜在的数据泄露风险点，并采取预防措施；

b） 泄露检测：部署数据泄露检测系统，实时监控数据访问和传输行为，及时发现异常；

c） 应急响应：制定数据泄露应急响应计划，一旦发现数据泄露，立即启动应急预案，控制泄露范围，减轻影响；

d） 通知机制：根据法律法规要求，在数据泄露发生后，及时向受影响的个人和监管部门通报情况；

e） 后续改进：对数据泄露事件进行深入分析，找出根本原因，优化数据保护措施，防止类似事件再次发生。

5.5 医疗数据分类分级管理

5.5.1 **数据分类体系：**医疗数据应按照以下维度进行分类：

5.5.1.1 按数据性质分类

a） 患者身份数据：姓名、身份证号、联系方式、住址等直接识别信息；

b） 临床诊疗数据：病历记录、诊断信息、处方医嘱、检验检查结果、手术记录等；

c） 医疗管理数据：挂号信息、收费记录、床位使用、药品库存等；

d） 科研教学数据：去标识化的病例资料、医学影像、基因组数据等；

e） 设备运行数据：医疗设备运行状态、维护记录、质控数据等；

f） 语音交互数据：医患对话录音、语音识别文本、语义分析结果等。

5.5.1.2 按数据来源分类

患者直接提供数据；医疗服务生成数据；第三方机构共享数据；物联网设备采集数据；公开渠道获取数据。

5.5.2 **数据分级标准：**

依据数据敏感程度和安全影响，将医疗数据分为四级：

a） 四级（极高敏感级）：包含患者直接识别信息的完整病历数据；涉及国家安全、社会稳定的

特殊病例数据；重大传染病暴发期间的疫情相关数据；未经脱敏的基因测序等生物特征数据；

b) 三级（高敏感级）：去标识化后的诊疗核心数据（诊断、治疗方案、检查结果）；医院运营管理中的关键数据（财务、人事、科研核心数据）；语音交互中的医患对话原始录音；

c) 二级（中敏感级）：统计汇总的医疗服务质量数据；设备运行状态与维护数据；脱敏后的科研教学病例数据；语音识别后的文本数据（已去除身份信息）；

d) 一级（低敏感级）：公开的医疗服务信息；匿名化的统计研究数据；医疗常识库、药品基础信息。

5.5.3 分级保护要求

a) 四级数据：必须存储在境内安全可控的专用存储区域，实施物理隔离、加密存储、多因素认证、全程操作审计，禁止跨境传输；

b) 三级数据：需加密存储，访问控制到用户级别，操作留痕，跨境传输需通过安全评估；

c) 二级数据：需身份认证和权限控制，重要操作可追溯；

d) 一级数据：基础安全防护，防止篡改和破坏；

e) 四级数据分类中的所有数据。

5.6 患者数据授权机制

5.6.1 授权基本原则

a) 知情同意：使用清晰易懂的语言告知患者数据使用目的、范围、期限等；

b) 自主选择：患者有权自主决定是否授权，且不因拒绝授权而影响基本医疗服务；

c) 最小必要：仅收集和使用与医疗服务直接相关的数据；

d) 动态管理：患者可随时查看、修改、撤回授权；

e) 特殊保护：对未成年人、无行为能力人等特殊人群建立代理授权机制。

5.6.2 授权层级设计

建立三级授权体系，满足不同场景需求：

a) 基础治疗授权（一级授权）：

范围：诊疗必需的病历查阅、检查检验、院内会诊；

特点：默认获得，但需明确告知患者，患者可明确拒绝；

有效期：单次就诊期间或连续治疗周期内。

b) 扩展应用授权（二级授权）：

范围：科研使用、质量改进、跨机构共享、保险理赔；

特点：需单独明确授权，可选择性同意部分用途；

有效期：患者指定期限，最长不超过 3 年。

c) 特殊用途授权（三级授权）：

范围：商业合作、跨境传输、基因研究等敏感用途；

特点：需单独书面（包括电子形式）授权，明确告知风险；

有效期：患者指定期限，需每年重新确认。

5.6.3 授权管理具体要求

5.6.3.1 授权获取

a） 区分“同意”与“授权”，重要数据使用需获得主动授权而非默认同意；

b） 采用分层呈现方式，先简要说明再提供详细条款；

c） 对重要条款（如数据共享、二次利用）采用增强告知方式；

d） 为听力、视力障碍者提供无障碍授权方式；

e） 紧急情况下可先行使用数据，但需在 48 小时内补办授权手续。

5.6.3.2 授权记录

a） 采用区块链等技术确保授权记录不可篡改；

b） 记录授权时间、内容、版本、患者身份验证信息；

c） 长期保存授权记录，至少保存至数据使用结束后 10 年。

5.6.3.3 授权变更与撤回

a） 提供便捷的授权管理入口，患者可随时查看当前授权状态；

b） 撤回授权应在 3 个工作日内生效，并通知所有数据接收方；

c） 撤回后，除法律要求保留的数据外，应停止使用并安全删除相关数据；

d） 对基于已撤回授权做出的决策，如涉及患者权益，应重新评估。

5.6.4 特殊情形处理

a） 未成年患者

8 周岁以下：由监护人完全代理授权；8-16 周岁：需获得患者本人及监护人共同授权；16-18 周岁且能辨认自己行为：可独立授权，但建议告知监护人；

b） 无行为能力患者：

由法定监护人代理授权，紧急情况下可由医疗机构负责人临时授权，事后补办手续；

c） 群体健康研究：

可采用广泛通知加选择退出机制，但需提供易于操作的退出渠道，对选择退出的患者数据应及时排除。

5.6.5 **语音数据特殊授权要求**：基于语音技术的应用需额外获得以下授权：

a） 语音采集的单独明确授权，告知录音范围、保存期限；

b） 语音识别处理的授权，告知可能的误识别风险；

c） 语音特征分析的授权，告知生物特征识别特性；

d） 提供实时静音和删除功能，患者可随时停止录音或删除已录内容。

5.7 数据安全管理措施

5.7.1 技术防护措施

a） 四级、三级数据存储加密强度不低于 SM4/AES-256 算法；

b） 建立数据防泄露系统，监控异常数据传输行为；

c） 语音数据存储时需分离存储音频文件和文本文件；

d） 重要操作采用生物特征或多因素认证；

e） 建立数据备份与灾难恢复机制，核心数据保留至少 3 个副本。

5.7.2 管理控制措施

a） 设立数据保护官职位，负责数据分类分级和授权管理；

b） 建立数据使用审批流程，高敏感数据使用需双重审批；

c） 定期进行数据安全审计和风险评估，每年至少一次；

d） 制定数据安全事件应急预案，半年进行一次演练；

e） 所有数据操作人员需签署保密协议并通过背景审查。

5.7.3 监测与审计

a） 建立全链路数据操作日志，保存时间不少于 6 年；

b） 对高敏感数据访问实施实时监控和异常预警；

c） 定期生成数据安全报告，向医院管理委员会汇报；

d） 接受卫生健康行政部门和网信部门的监督检查。

5.8 责任与监督

5.8.1 责任主体

a） 医院法定代表人是数据安全第一责任人；

b） 数据保护官负责具体数据管理工作的组织实施；

c） 各科室负责人负责本科室数据管理制度的执行；

d） 信息系统供应商需承担技术保障责任。

5.8.2 违规处理

a） 违反数据分类分级规定的，视情节给予警告、通报批评；

b） 未经授权跨境传输数据的，依法追究法律责任；

c） 侵犯患者数据权利的，承担相应民事赔偿责任；

d） 造成严重后果的，依法追究相关人员的刑事责任。

5.8.3 监督机制

a） 医院内部设立数据安全监督委员会；

b） 定期向患者公布数据保护情况报告；

c） 建立患者投诉渠道，15 个工作日内反馈处理结果；

d） 接受卫生健康、网信、公安等部门的联合监管。

6. 智能语音技术

6.1 语音技术在医疗领域的应用场景

语音技术在医疗领域的具体应用包括但不限于以下几个方面：

6.1.1 电子病历记录：医生通过语音识别技术口述病历或影像阅片技师口述检查所见，系统自动转换成文字记录。

6.1.2 智能导诊系统：利用语音识别技术，就诊人群通过语音与系统交互，获取就医指导和相关信息。

6.1.3 药物信息查询系统：语音技术辅助医生或药师查询药物信息，避免用药错误，确保就诊人群用药安全。

6.1.4 远程医疗咨询：医生通过语音交互系统远程为就诊人群提供咨询服务。

6.2 语音识别与合成技术标准

6.2.1 语音识别技术标准

a) 准确性标准：语音识别技术需要达到高准确率，以减少医疗差错；

b) 实时性标准：语音交互系统应具备快速响应能力，以适应医疗场景中的紧急需求；

c) 隐私保护标准：医疗数据涉及就诊人群隐私，语音技术必须符合数据保护法规，确保信息安全；

d) 用户适应性标准：系统应能够适应不同口音和语速的语音输入，将医护人员或患者的口语化表达识别为标准化的医学术语。

6.2.2 语音合成技术标准

a) 自然度：合成语音应尽可能接近人类自然语音，包括语调、节奏、情感表达等；

b) 可理解性：听众应能够轻松理解合成语音的内容，不受发音错误或不清晰的语音影响；

c) 多样性：系统应支持多种声音类型，包括不同性别、年龄、语言和方言的声音；

d) 定制性：用户应能够根据需要定制语音的参数，如语速、音量、音调等；

e) 多语言和方言支持：系统能支持多语言和方言的语音合成。

6.3 语音交互系统设计与评估

6.3.1 系统设计原则

a) 用户中心设计：系统设计应以用户需求为中心，确保系统易于使用，满足医疗工作者和就诊人群的需求；

b) 多模态交互：结合语音、触屏等多种交互方式，提供更丰富的用户体验；

c) 可扩展性：系统设计应考虑未来的技术升级和功能扩展，保持系统的长期适用性。

6.3.2 系统评估方法

a) 客观评估：通过技术指标如准确率、响应时间等来评估系统性能；

b) 主观评估：通过用户调查和反馈来评估系统的易用性、满意度等；

c) 任务完成率：衡量用户通过系统完成特定任务的成功率；

d) 用户参与度：评估用户与系统的交互频率和深度；

e) 错误分析：识别和分析系统在交互过程中出现的错误，以及这些错误对用户体验的影响；

f) 可用性测试：通过实际用户在受控环境中使用系统来发现潜在的问题和改进点。

7. 智能平台功能要求

7.1 临床护理支持功能应包括

7.1.1 就诊人群监护：通过集成的传感器和监测设备，实现对就诊人群生命体征的实时监控和数据分析。

7.1.2 药物管理：智能提醒系统确保药物按时准确分发，同时利用大数据分析优化药物库存管理。

7.1.3 护理记录：电子化护理记录系统，便于信息共享和历史数据追踪，提高护理文档的准确性和完整性。

7.2 就诊人群服务与管理功能包括

7.2.1 智能导诊：利用自然语言处理技术，提供智能分诊和就医指导服务，缩短就诊人群等待时间。

7.2.2 就诊人群教育：通过语音交互技术，提供疾病预防、治疗和康复的相关知识，增强就诊人群自我管理能力。

7.2.3 随访管理：自动化随访系统，根据就诊人群病情和治疗计划，定期提醒就诊人群复查和随访。

7.3 医疗质量管理功能包括

7.3.1 质量监控：实时收集医疗服务数据，通过数据分析发现潜在的质量问题，及时进行干预。

7.3.2 风险评估：利用机器学习算法，对医疗过程中的风险因素进行评估和预测，减少医疗差错。

7.3.3 持续改进：基于质量监控和风险评估的结果，制定改进措施，持续提升医疗服务质量。

7.4 后勤与资源管理

后勤与资源管理功能涉及

7.4.1 物资管理：智能平台通过物联网技术，实现医疗物资的实时追踪和管理，优化库存控制。

7.4.2 设备维护：预测性维护系统，通过分析设备使用数据，预测设备故障，减少意外停机时间。

7.4.3 能源管理：智能监控医院能源使用情况，通过优化能源分配和使用，降低运营成本。

8.技术标准与协议

8.1 技术接口标准

8.1.1 接口定义与规范

技术接口是医院智能平台与外部系统进行交互的桥梁。接口定义应遵循开放标准，如 RESTful API 或 SOAP，以确保不同系统间的互操作性。接口规范应详细描述请求和响应的数据结构、编码方式、认证机制等，以便于开发者理解和使用。

接口定义应包括：请求方法（GET, POST, PUT, DELETE 等）、请求 URL 和参数、请求和响应的数据格式（JSON, XML 等）、认证和授权机制、错误处理和返回码。

8.1.2 安全性与兼容性要求

安全性是技术接口的重要考虑因素。接口应实现数据加密传输（如使用 HTTPS 协议），并提供身份验证和授权机制，以防止未授权访问和数据泄露。同时，接口应有防止 SQL 注入、跨站脚本攻击（XSS）等网络安全措施。

兼容性要求确保接口能够适应不同操作系统和开发环境。接口应支持主流编程语言和平台，如 Java、Python、.NET 等，并考虑到移动设备和桌面应用的接入需求。

8.1.3 接口版本管理与迭代

随着医院智能平台的发展，接口可能会进行更新和迭代。合理的版本管理策略对于维护系统的稳定性和向后兼容性至关重要。接口版本应明确标识，并提供版本更新日志，记录变更点和升级指南。

迭代过程中，应考虑向下兼容，避免因更新导致的第三方应用中断。同时，应提供废弃接口的过渡期，给予开发者足够的时间进行适配。

8.2 数据交换格式与协议

数据交换格式是信息在系统间传递的基础。常见的数据交换格式包括 JSON、XML 等，它们具有结构化和易于解析的特点。选择数据交换格式时，应考虑数据的复杂性、传输效率和解析成本。

数据交换协议应定义：数据模型和结构、必填字段和可选字段、数据类型和格式（日期、时间、数值等）、错误处理机制。

8.2.1 数据结构标准选择

a) HL7 FHIR（Fast Healthcare Interoperability Resources）：作为 HL7 的最新规范，FHIR 通过 RESTful API 简化了医疗信息的交换，支持了移动设备和云计算的发展；

b) DICOM（Digital Imaging and Communications in Medicine）：特别针对医疗影像数据的标准化，DICOM 标准确保了不同影像设备生成的数据能够在平台上无缝集成和分析。

8.2.2 通信协议选择

a) MQTT（Message Queuing Telemetry Transport）：适用于需要低带宽、高实时性的场景，如远程监控和设备通信；

b) AMQP（Advanced Message Queuing Protocol）：支持复杂的消息路由和队列，适用于需要高可靠性和灵活路由的系统；

c) CoAP（Constrained Application Protocol）：为物联网设备设计，适用于资源受限的环境。

8.2.3 数据加密与完整性保护

a) 使用 AES（Advanced Encryption Standard）算法对存储和传输的数据进行加密，确保数据的机密性；

b) 利用 HMAC（Hashbased Message Authentication Code）算法进行消息认证，防止数据在传输过程中被篡改；

c) 实施定期的安全审计和漏洞扫描，确保系统的安全性，并及时更新加密算法和协议以应对新的安全威胁。

此外，平台应支持数据的完整性校验，如使用数字签名技术，确保数据在传输和存储过程中未被篡改，维护数据的原始性和可信度。

8.3 数据兼容性与扩展性

数据兼容性确保新旧系统能够无缝交换数据。在设计数据模型时，应考虑未来可能的变更和扩展，采用模块化和松耦合的设计原则。

兼容性与扩展性策略包括：使用抽象和泛化来设计数据模型、提供扩展点和钩子，允许第三方开

发者添加自定义功能、维护向后兼容性，确保旧版本系统能够与新版本系统交换数据。

8.3.1 **兼容性保障机制**：数据兼容性是医院智能平台建设中的关键因素，它确保了不同系统和设备之间的无缝交互和数据共享。

a) 标准化协议：采用国际通用的数据交换标准，如 HL7 和 FHIR，以确保不同系统间的通信和数据交换；

b) 中间件技术：使用中间件作为不同系统间的桥梁，它可以转换和适配不同格式的数据，以实现兼容；

c) 数据映射：对不同来源的数据进行映射，确保数据字段和结构的一致性，从而减少数据转换过程中的错误和歧义。

8.3.2 **系统扩展性设计原则**

a) 模块化设计：将系统分解为独立的模块，每个模块负责特定的功能，这样可以在不影响其他模块的情况下更新或替换单个模块；

b) 服务导向架构（SOA）：采用 SOA 原则，将业务功能封装成服务，便于不同应用之间的集成和重用；

c) 微服务架构：通过微服务架构，将大型应用拆分成小型、独立的服务，这些服务可以独立部署、扩展和更新。

9 用户界面与交互设计

9.1 设计原则与理论基础

9.1.1 **以用户为中心的设计**

以用户为中心的设计理念（User-Centered Design, UCD）强调在设计过程中始终将用户的需求和体验放在首位。在医院智能平台的用户界面设计中，这意味着需要深入理解医护人员、就诊人群及其家属的使用习惯、任务需求和心理模型。

9.1.2 **一致性与直观性**

a) 设计标准：制定一套界面设计标准，包括颜色、字体、布局和控件的使用，以保持界面的一致性；

b) 直观性设计：通过使用熟悉的图标、隐喻和布局，提高界面的直观性，帮助用户快速识别和操作。

9.1.3 **反馈与错误预防**

a) 操作反馈：确保每次用户操作都有明确的反馈，如按钮点击效果、操作成功的提示等；

b) 错误处理：设计清晰的错误提示信息，并提供错误恢复的途径，减少用户的操作困扰。

9.2 交互流程优化

9.2.1 **任务分析与流程设计**

a) 任务模型：构建任务模型，明确用户目标和完成任务的步骤；

b) 流程优化：通过简化步骤、减少操作和等待时间来优化用户任务流程。

9.2.2 交互模式与用户行为预测

交互模式的设计应基于对用户行为的预测和理解。

a) 交互模式：设计符合用户预期的交互模式，如触控、语音、手势等；

b) 用户行为分析：利用数据分析和机器学习技术预测用户行为，为交互设计提供依据。

9.2.3 多模态交互设计

a) 感官整合：设计时考虑不同感官通道的协同作用，如视觉指示与听觉反馈的结合；

b) 情境适应性：根据用户所处的环境和任务需求，提供适应性的多模态交互方式。

9.3 用户体验评估与提升

9.3.1 用户体验度量指标

a) 度量指标：定义可用性、效率、满意度等关键指标，用于评估用户体验；

b) 数据收集：通过日志分析、在线调查、实验室测试等方法收集用户体验数据。

9.3.2 可用性测试与用户反馈分析

a) 测试方法：运用启发式评估、认知漫步、A/B 测试等方法进行可用性测试；

b) 反馈机制：建立有效的用户反馈收集和分析机制，及时响应用户需求。

9.3.3 个性化与适应性设计策略

a) 个性化设置：允许用户根据自己的偏好设置界面布局、颜色主题等；

b) 适应性交互：根据用户的行为和上下文信息，智能调整交互方式和内容呈现。

10 质量控制与评估

10.1 质量控制流程

10.1.1 定义与目标

质量控制流程是确保医院智能平台建设与语音技术应用达到预期效果的关键环节。其定义为一系列系统化的活动，旨在监控和指导项目实施过程，确保输出符合既定的质量标准。目标是通过持续监控和评估，提升智能平台的稳定性、准确性和用户满意度。

10.1.2 流程设计原则

a) 系统性：确保流程覆盖平台建设的每个环节；

b) 预防为主：通过预先设定标准，防止质量问题的发生；

c) 数据驱动：利用数据分析来指导质量控制决策；

d) 用户参与：确保用户需求和反馈被纳入质量控制流程。

10.1.3 实施步骤

a) 明确质量标准和指标；

b) 设计质量控制检查点；

c) 制定检查清单和评估工具；

d) 培训相关人员；

e) 执行质量检查并记录结果；

f） 分析问题原因并制定改进措施；

g） 跟踪改进效果并进行循环。

10.2 性能评估标准

10.2.1 评估指标体系构建要求

a） 准确性：智能平台处理医疗信息的准确度；

b） 响应时间：系统响应用户请求的速度；

c） 用户满意度：用户对平台使用体验的满意程度；

d） 系统稳定性：系统运行的可靠性和故障率；

e） 安全性：数据保护和隐私安全措施的有效性。

10.2.2 指标权重确定方法

a） 专家咨询：邀请领域专家对各指标的重要性进行评分；

b） 数据分析：基于历史数据和用户反馈分析各指标的相关性和影响力；

c） 德尔菲法：通过多轮问卷调查，收集并整合专家意见。

10.2.3 评估流程

a） 设定评估计划和时间表；

b） 选择或开发评估工具；

c） 收集数据并进行分析；

d） 根据评估结果进行排名和分类；

e） 形成评估报告并提出改进建议。

10.3 持续改进机制

10.3.1 问题识别方法

a） 定期审查：周期性地检查质量控制报告；

b） 用户反馈：收集和分析用户的使用反馈；

c） 故障报告：记录和分析系统故障和用户错误报告。

10.3.2 改进措施的制定与实施

a） 基于问题识别的结果，确定改进的优先级和方向；

b） 制定具体的改进计划和实施步骤；

c） 分配资源并监督改进措施的执行。

10.3.3 改进效果的监测与评估

a） 设定改进效果的评估标准和指标；

b） 定期跟踪改进措施的执行情况和效果；

c） 根据监测结果调整改进策略，确保持续改进的循环。

10.4 运维期质量管理与责任分工

10.4.1 总体原则

平台投入运行后，应遵循“权责清晰、协同高效、安全可控、持续改进”的原则，建立由医院方与外部供应商、厂商共同参与的运维管理体系。双方应在服务协议或合同中明确界定运维责任边界、服务等级协议（SLA）、响应流程及考核标准。

10.4.2 责任边界界定

医院方与外部厂商的运维责任应根据平台建设模式（如自建、采购、合作开发等）及系统部署方式（如本地化部署、云端部署、混合部署）进行具体划分，但至少应明确以下核心边界：

10.4.2.1 医院方主要职责

a) 内部管理与协调：负责平台日常运营的统筹管理，内部业务部门的协调，以及最终用户的使用培训与支持；

b) 基础环境保障：保障平台运行所必需的机房、电力、网络（院内部分）等基础设施的稳定与安全；

c) 数据管理与安全主体责任：作为医疗数据的所有者与管理者，负责数据的产生、录入、审核、归档、备份策略制定及数据安全管理的最终责任。确保数据使用符合伦理规范与隐私保护要求；

d) 业务合规性监督：监督平台各项功能在临床、管理、科研等场景中的应用符合医疗规范、行业政策及法律法规；

e) 厂商履约监督：依据协议对厂商提供的运维服务进行监督、考核与验收。

10.4.2.2 外部厂商主要职责

a) 平台技术保障：负责平台软件本身（包括大模型算法、应用模块、接口等）的稳定性、性能优化、缺陷修复、版本升级及技术演进支持；

b) 专项技术服务：提供与平台紧密相关的技术运维服务，包括但不限于：大模型微调与优化支持、语音识别引擎的维护与更新、核心算法的迭代、专用知识库的维护支持等；

c) 部署环境技术支持（根据合同约定）：若为云端服务或包含硬件设备，厂商需负责云资源/硬件设备的监控、维护、扩容及基础运行环境保障。若为本地化部署，双方应明确操作系统、中间件、数据库等基础软件的维护责任方；

d) 接口与集成维护：负责平台与外部系统（如 HIS、EMR 等）接口的技术维护，确保数据交换的稳定与准确；

e) 技术支持响应：建立针对不同严重等级问题的技术支持通道，提供远程或现场技术服务。

10.4.3 故障应急处理机制

应建立分级分类的故障应急处理流程，确保故障发生时能快速响应、有效处置。

10.4.3.1 故障分类与定级：

根据故障对业务的影响范围、严重程度（如：系统完全瘫痪、关键功能失效、性能严重下降、一般性功能异常等）和持续时长，明确划分故障等级（如：一级/重大、二级/严重、三级/一般）。

10.4.3.2 应急响应流程

a) 报告与受理： 建立统一的故障受理入口（如医院信息科），由医院方初步判断并通知相关责任方；

b) 诊断与定责： 医院方与厂商协同进行故障诊断，快速确定故障点及首要责任方。对于责任边界模糊的故障，应以恢复业务为优先，事后根据协议界定；

c) 处置与恢复： 根据故障等级，启动相应预案。首要责任方牵头处置，另一方积极配合。明确各级故障的目标恢复时间（RTO）和数据恢复点目标（RPO）；

d) 升级与通报： 对于高等级故障或处置超时情况，应建立管理层级通报与协调机制。必要时，启动由院领导牵头的应急指挥小组；

e) 事后分析与改进： 故障解决后，责任方应出具书面故障分析报告，内容包括原因分析、处置过程、责任认定（如适用）及预防改进措施。医院方应组织复盘，持续优化流程。

10.4.3.3 应急预案与演练：

针对可能出现的重大故障场景（如数据中心故障、核心数据库损坏、大规模网络攻击等），制定详细的应急预案，并定期组织跨部门的联合演练。

10.4.4 运维质量持续评估

应建立运维服务质量的量化评估与持续改进机制。

a) 关键绩效指标（KPI）： 制定涵盖系统可用性、故障发生率、平均修复时间（MTTR）、服务请求响应与解决满意度、安全事件数量等方面的 KPI 指标；

b) 定期评审： 医院方应会同厂商定期（如每季度或每半年）召开运维服务评审会，基于 KPI 数据、故障记录、用户反馈等评估运维质量，审议改进计划；

c) 持续改进： 根据评审结果和业务发展需要，不断优化运维流程、技术架构及服务内容，推动平台运维管理水平的持续提升。

11 临床责任与风险管理

11.1 总则

11.1.1 适用范围

本章适用于基于大模型的医院智能平台在临床诊疗、辅助决策、患者咨询等涉及医疗核心业务场景中的风险管理与责任界定。

11.1.2 核心原则

a) 人类中心原则：人工智能系统作为辅助工具，最终临床决策权必须由执业医师掌握；

b) 风险控制原则：建立多层防御机制，预防、识别和缓解大模型幻觉风险；

c) 可追溯原则：所有模型输出、人工审核、最终决策必须完整记录、可追溯；

d) 责任明确原则：明确划分技术提供方、医疗机构、临床医师的责任边界。

11.2 大模型幻觉风险控制机制

11.2.1 幻觉风险分类与等级

根据风险严重程度，将大模型幻觉风险分为四级

11.2.1.1 一级风险（极高风险）

a) 生成完全虚构的疾病诊断；

b) 推荐禁忌药物或治疗方案；

c) 伪造实验室检查结果；

d) 提供危及生命的错误医疗建议。

11.2.1.2 二级风险（高风险）

a) 夸大或低估疾病严重程度；

b) 提供不完整的鉴别诊断；

c) 推荐次优治疗方案；

d) 药物剂量计算错误。

11.2.1.3 三级风险（中风险）

a) 引用过时或未被广泛接受的医学知识；

b) 对罕见病给出确定性过高的判断；

c) 忽略患者个体差异的标准化建议；

d) 医学术语使用不准确。

11.2.1.4 四级风险（低风险）

a) 语言表述不够严谨但无实质错误；

b) 非核心信息的轻微不准确；

c) 格式或呈现方式不符合临床习惯。

11.2.2 幻觉预防技术措施

11.2.2.1 输入验证机制

a) 对输入临床数据实施完整性校验；

b) 识别并拦截异常、矛盾或超出合理范围的输入；

c) 建立医学知识边界约束，限制模型生成范围。

11.2.2.2 输出约束机制

a) 设置置信度阈值，低置信度输出必须触发人工复核；

b) 实施事实性核查，自动比对权威医学知识库；

c) 建立输出格式模板，强制关键信息结构化呈现；

d) 对数字、剂量、时间等关键信息实施双重计算验证。

11.2.2.3 确定性表达

a) 模型必须明确标注其知识截止日期；

b) 对推断性内容必须标注置信度水平；

c) 提供备选方案时需说明证据等级；

d) 区分“事实陈述”与“建议参考”。

11.2.2.4 持续监测系统

a) 实时监控模型输出的异常模式；

b) 建立幻觉风险预警指标体系；

c) 对高风险科室（如急诊、ICU）实施加强监控；

11.3 临床责任边界与决策流程

11.3.1 大模型输出法律地位

a) 大模型生成的任何医疗建议、诊断提示、治疗方案均视为参考信息，不具备法律效力；

b) 模型输出不得直接呈现给患者作为诊疗结论；

c) 模型输出不得替代任何法定医疗文书；

d) 模型输出不能作为医疗事故鉴定中的独立证据。

11.3.2 临床决策责任链条

11.3.2.1 第一责任人：执业医师

a) 对最终诊疗决策承担全部法律责任。

b) 必须独立审查模型输出的合理性和适用性；

c) 有权拒绝采纳模型建议，需在系统中记录理由；

d) 不得以“系统建议”为由免除个人专业判断责任。

11.3.2.2 第二责任人：医疗机构

a) 建立合理的模型使用流程和审核制度；

b) 提供必要的培训，确保医务人员正确理解系统局限性；

c) 维护系统运行环境，确保技术可靠性；

d) 建立医疗风险分担机制。

11.3.2.3 第三责任人：技术提供方

a) 确保模型训练数据的质量和代表性；

b) 持续优化模型，降低幻觉发生频率；

c) 提供准确、透明的模型性能指标；

d) 建立技术故障应急响应机制。

11.3.3 强制性人工复核流程

11.3.3.1 必须复核的情形

a) 初诊患者的首次模型辅助诊断；

b) 涉及重大治疗决策（手术、化疗、放疗等）；

c) 模型给出的罕见病或疑难病诊断；

d) 模型推荐治疗方案与常规实践差异显著；

e) 模型置信度低于预设阈值；

f) 患者病情突然变化后的模型重新评估。

11.3.3.2 复核记录要求

a) 记录复核开始时间、结束时间；

b) 明确标注采纳、修改或拒绝模型建议；

c) 如修改或拒绝，必须详细说明理由；

d) 复核记录需电子签名并归档保存。

11.4 追溯机制与日志管理

11.4.1 全链路追溯要求

11.4.1.1 输入追溯

a) 记录完整的输入数据来源、时间、版本；

b) 患者身份匿名化标识，满足隐私保护要求；

c) 临床数据更新时间戳和提供者信息。

11.4.1.2 处理追溯

a) 记录模型调用时间、版本、参数配置；

b) 保存中间推理过程关键节点（如知识检索记录）；

c) 记录参考的知识来源及引用片段。

11.4.1.3 输出追溯

a) 完整保存原始输出内容和格式；

b) 标注系统自动评估的置信度分数；

c) 记录输出到各终端的分发情况。

11.4.1.4 人工交互追溯

a) 记录医师查看、编辑、批注的全过程；

b) 保存最终采纳的版本及修改痕迹；

c) 记录不同医务人员之间的协作审阅流程。

11.4.2 日志留存规范

11.4.2.1 留存内容

a) 完整的输入输出数据包（加密存储）；

b) 系统性能指标（响应时间、资源使用）；

c) 用户操作序列（查询、修改、确认、拒绝）；

d) 人工复核的详细记录和签名；

e) 系统异常和错误事件报告。

11.4.2.2 留存期限

a) 涉及诊疗决策的关键日志：永久保存；

b) 一般性咨询交互日志：不少于患者就诊后 30 年；

c) 系统运行技术日志：不少于 10 年；

d) 安全审计日志：不少于6年。

11.4.2.3 存储要求

a) 采用防篡改技术（如区块链、数字签名）；

b) 异地灾备，至少三个地理分散的副本；

c) 定期完整性校验，每年至少一次；

d) 加密存储，访问权限最小化原则。

11.5 错误处置与持续改进

11.5.1 错误识别与报告

11.5.1.1 错误分类

A类：可能导致严重医疗后果的错误；

B类：可能影响治疗效果但不危及生命的错误；

C类：表述不准确但不影响核心医疗决策的错误；

D类：系统性能或可用性问题。

11.5.1.2 报告流程

a) 一线医务人员发现错误，24小时内报告科室质量管理员；

b) A类错误必须立即报告，并启动紧急处置程序；

c) 建立匿名报告渠道，鼓励错误信息上报；

d) 错误报告不得作为处罚依据，除非涉及故意隐瞒。

11.5.2 根因分析与系统改进

11.5.2.1 分析机制

a) 成立多学科错误分析小组（临床、技术、管理）；

b) 区分技术性幻觉、知识缺陷、流程漏洞等不同类型；

c) 建立错误案例库，标注根本原因和改进措施。

11.5.2.2 改进措施

a) 技术性幻觉：优化模型架构、增强事实核查；

b) 知识缺陷：更新知识库、调整训练数据分布；

c) 流程问题：修改操作流程、加强人员培训；

d) 高频错误场景：建立专项预警和拦截规则。

11.5.2.3 闭环管理

a) 错误报告必须在30天内反馈处理进展；

b) 重大错误改进措施需在90天内实施验证；

c) 定期发布错误分析和改进报告（每季度）。

11.6 法律责任与风险分担

11.6.1 责任划分标准

11.6.1.1 技术提供方责任

a) 因模型算法缺陷导致的系统性错误；

b) 未披露已知的系统局限性；

c) 安全漏洞导致的数据泄露或系统被恶意利用；

d) 未达到承诺的性能指标。

11.6.1.2 医疗机构责任

a) 未建立合理的人工复核流程；

b) 未对医务人员进行必要培训；

c) 在已知系统缺陷情况下仍强制推广使用；

d) 管理漏洞导致错误决策未被及时发现。

11.6.1.3 医务人员责任

a) 未进行必要的人工审核即采纳模型建议；

b) 明显错误未识别或未采取纠正措施；

c) 超出授权范围使用系统功能；

d) 故意利用系统漏洞或提供误导性输入。

11.6.2 风险分担机制

11.6.2.1 医疗责任保险

a) 技术提供方需购买产品责任险，保额不低于 5000 万元；

b) 医疗机构应将 AI 辅助诊疗纳入医疗责任险范围；

c) 保险条款需明确覆盖人工智能相关风险。

11.6.2.2 技术风险披露

a) 在系统显著位置提示潜在风险和局限性；

b) 向医务人员提供完整的风险告知书；

c) 记录每位医务人员接受风险培训的情况。

11.6.2.3 患者知情同意

a) 使用 AI 辅助诊疗前需获得患者特别知情同意；

b) 同意书中需说明 AI 的作用、局限性和人工审核机制；

c) 患者有权拒绝使用 AI 辅助，不影响获得标准医疗服务。

11.6.3 纠纷处理机制

11.6.3.1 内部处理程序

a) 设立 AI 医疗纠纷专门调解小组；

b) 优先通过调解方式解决争议；

c) 完整提供系统日志作为证据材料。

11.6.3.2 第三方鉴定

a) 建立由医学、法律、技术专家组成的鉴定专家库；

b) 开发专门的 AI 医疗决策过程分析工具；

c) 鉴定重点：人工审核是否充分、流程是否合规。

11.6.3.3 法律适用

a) 优先适用《医疗器械监督管理条例》等专门法规；

b) 参考《中华人民共和国产品质量法》《中华人民共和国民法典》相关规定；

c) 最高人民法院发布的相关司法解释。

11.7 培训与考核

11.7.1 医务人员培训要求

11.7.1.1 培训内容

a) 大模型基本原理和局限性（不少于 4 学时）；

b) 幻觉风险识别与处理方法（不少于 4 学时）；

c) 系统操作与审核流程实操训练（不少于 8 学时）；

d) 相关法律法规和伦理规范（不少于 4 学时）。

11.7.1.2 培训对象：

a) 所有使用系统的临床医师：强制培训；

b) 相关医技、护理人员：推荐培训；

c) 医疗质量管理人员：强制培训；

d) 医院信息技术人员：专业培训。

11.7.2 考核与授权

11.7.2.1 考核标准

a) 理论考试：正确率不低于 90%；

b) 实操评估：能正确识别和处置典型幻觉案例；

c) 情景模拟：符合临床审核流程规范。

11.7.2.2 授权管理

a) 考核合格后获得系统使用授权；

b) 授权有效期 2 年，需定期复训；

c) 分级授权：初级用户有限功能，高级用户全功能；

d) 发生严重审核失误的，暂停或取消授权。

11.7.2.3 持续教育

a) 每季度更新培训内容，反映系统改进和最新风险；

b) 每月发布典型案例分析，供医务人员学习；

c) 建立经验分享平台，鼓励最佳实践交流；

d) 将 AI 系统使用能力纳入医务人员继续教育学分。

参考文献

[1]《信息安全技术—个人信息安全规范》

[2]《信息安全技术—健康医疗数据安全指南》

[3]湖北省加快推进人工智能在医疗卫生领域应用工作实施方案（2025—2027 年）

[4]《人工智能医疗器械 质量要求和评价 第 3 部分：数据标注通用要求》

[5]《新一代人工智能伦理规范》