ICS 35.020
CCS L70

团 体 标 准

T/ISC XXXX—XXXX

医学影像大模型技术要求

Technical requirements for medical imaging large models

（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：安徽省合数智医科技有限公司、讯飞医疗科技股份有限公司、安徽讯飞影联科技有限公司、中国信息通信研究院

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：

——

医学影像大模型技术要求

1 范围

本文件规定了医学影像大模型的技术要求，包括通用性功能要求、接口要求、性能要求和安全要求。

本文件适用于各级医疗机构、医疗AI企业、科研机构、监管机构及生态合作伙伴等相关单位的医学影像大模型的规划、设计、建设、研发、测试、部署、运维、迭代优化及相关技术应用。

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 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

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 39725-2020 信息安全技术 健康医疗数据安全指南

3 术语和定义

3.1

医学影像大模型 medical imaging large model

基于国产化算力基础设施与自主可控大模型底座，针对医学影像领域研发，具备全模态影像处理、辅助诊断、质控管理、科研支撑、知识迭代等能力的人工智能模型。

3.2

全模态数据处理 full-modal data processing

对CT、MRI、X光、超声、病理切片等各类医学影像，及文本、生理信号等多元临床数据进行统一接入、预处理与融合分析的技术过程。

3.3

细粒度病灶分析 fine-grained lesion analysis

对微小病灶、边界模糊病灶进行精准定位，并开展量化研判的分析方式。

3.4

结构化报告生成 structured report generation

依据医疗文书规范与医学编码标准，自动提取诊断信息，生成标准化、可编辑、可追溯的医学影像报告的过程。

3.5

联邦学习 federated learning

在保障各机构数据隐私前提下，实现多中心数据协同训练、模型能力共享，做到数据“可用不可见”的分布式机器学习技术。

3.6

增量学习 incremental learning

在不破坏模型原有知识的基础上，融入新病例、新知识实现模型持续迭代优化的学习机制。

3.7

思维树 tree of thoughts

思维树是基于大模型的结构化多路径推理增强技术，为思维链线性推理的进阶范式。该技术将医学影像分析、病灶研判、诊断推理等复杂层级化任务拆解为树状推理分支，通过多节点思路生成、路径评

估与无效分支剪枝，择优输出最优推理结果，可有效提升医学影像大模型复杂场景推理的全面性、准确性与可解释性。

4 符号和缩略语

下列符号和缩略语适用于本文件。

AI：人工智能（Artificial Intelligence）
API：应用程序编程接口（Application Programming Interface）
AES：高级加密标准（Advanced Encryption Standard）
CT：计算机断层扫描（Computed Tomography）
DICOM：医学数字成像和通信（Digital Imaging and Communications in Medicine）
GPU：图形处理器（Graphics Processing Unit）
HIS：医院信息系统（Hospital Information System）
HL7：健康级别七（Health Level Seven）
FHIR：快速医疗互操作性资源（Fast Healthcare Interoperability Resources）
ICD-10：国际疾病分类 第十次修订本（International Classification of Diseases, 10th Revision）
IDS：入侵检测系统（Intrusion Detection System）
IPS：入侵防御系统（Intrusion Prevention System）
LIS：实验室信息系统（Laboratory Information System）
MRI：磁共振成像（Magnetic Resonance Imaging）
OAuth：开放授权（Open Authorization）
PACS：影像归档和通信系统（Picture Archiving and Communication Systems）
QPS：每秒查询率（Queries Per Second）
RBAC：基于角色的访问控制（Role-Based Access Control）
RIS：放射信息系统（Radiology Information System）
ROI：感兴趣区（Region of Interest）
RPO：恢复点目标（Recovery Point Objective）
RTO：恢复时间目标（Recovery Time Objective）
SDK：软件开发工具包（Software Development Kit）
SNOMED CT：医学临床术语系统命名法（Systematized Nomenclature of Medicine -- Clinical Terms）
TLS：传输层安全（Transport Layer Security）
VPN：虚拟专用网络（Virtual Private Network）
X光（DR/CR）：直接数字化X线摄影/计算机X线摄影（Digital Radiography/Computed Radiography）

5 通用性功能要求

5.1 全模态数据处理功能要求

5.1.1 多模态数据兼容要求

为保障模型适配各类医学影像及临床数据场景，实现多源数据无缝接入，本节针对数据兼容能力提出具体要求：

a) 应全面支持 CT、MRI、X 光（DR/CR）、超声、病理切片等主流影像模态，以及 MRI 的 T1、T2、DWI、FLAIR 等同一模态下多序列数据的无缝接入与协同处理；
b) 应支持完美兼容 DICOM 3.0、NIfTI、PNG 等主流医学影像格式，支持对不同设备厂商影像数据的标准化解析与格式转换；
c) 应支持具备文本（电子病历、检查申请单、医嘱）、生理信号（心电、血氧、血压）等多元数据的协同处理能力，支持多源数据关联融合。

5.1.2 自动化数据预处理要求

为提升影像数据处理效率、保障数据质量与隐私合规，实现全流程自动化预处理，本节提出具体要求：

a) 应支持内置模态特定预处理模块，可自动完成影像去噪、分辨率标准化、灰度校正等操作，预处理效果需通过放射科专家验证；
b) 应支持实现患者信息全流程去标识化处理（去除姓名、身份证号、住院号等个人敏感信息），支持数据脱敏效果验证，确保数据隐私保护合规。

5.1.3 跨模态信息融合要求

为打破异构数据壁垒，实现多模态信息深度融合与综合研判，提升复杂病例分析能力，本节提出具体要求：

a) 应支持构建全模态统一编码框架，通过注意力机制与对比学习，将异构影像数据映射至统一语义表征空间，实现多模态信息的有效对齐；
b) 应支持通过跨模态对比学习与互补信息挖掘，提升复杂病例（如多系统疾病、早期肿瘤）的综合研判能力，输出多模态融合分析结论；
c) 应支持多模态数据时序分析，可对同一患者不同时期的影像数据进行对比，适用于疾病进展监测、治疗效果评估与预后预测场景。

5.2 诊断辅助功能要求

5.2.1 细粒度病灶分析要求

为实现病灶精准定位与深度分析，提升早期病变与疑难病灶的识别准确率，本节针对病灶分析能力提出具体要求：

a) 应支持具备微小病灶、边界模糊病灶的精准定位能力，支持量化分析；
b) 应支持可有效区分“同病异影、异病同影”场景下的细微特征差异（如良恶性肿瘤的密度 / 信号差异），提升鉴别诊断准确性；
c) 应支持自动输出病灶位置、大小、密度 / 信号特征、强化方式等结构化描述信息，支持可视化展示（如叠加图层）。

5.2.2 全模态协同诊断要求

为整合多维度临床数据实现智能辅助决策，兼顾诊断科学性与可解释性，支撑医生精准诊疗，本节提出具体要求：

a) 应支持融合多模态影像及临床文本、生理信号等数据进行综合推理，输出鉴别诊断清单（含疾病名称、病灶等级及循证医学依据；
b) 应支持提供相似病例参考功能，自动检索病例库中匹配度最高的病例，辅助医生决策；
c) 应支持在鉴别诊断、用药推荐、手术方案设计、随访计划制定等环节提供实时临床决策建议，建议需关联权威临床指南或专家共识；
d) 应支持具备模型可解释性功能，展示诊断结论的推导过程，增强医生对诊断结果的信任度。

5.2.3 结构化报告生成要求

为规范医学影像报告撰写、提升报告流转效率，实现报告标准化与可追溯，本节提出具体要求：

a) 应支持自动提取核心诊断信息，生成符合医疗文书规范的结构化报告，内容涵盖检查部位、影像表现、诊断结论、建议等模块，支持医生二次编辑与修改；
b) 应支持报告模板自定义，可适配不同医院、不同专科（如胸部放射科、神经放射科）的报告书写习惯，提供模板导入 / 导出功能；
c) 应支持实现报告术语标准化，严格遵循 ICD－10 疾病分类标准、SNOMED CT 医学术语编码规范，支持报告数据结构化存储与统计分析；
d) 应支持报告自动排版、打印、电子签名及与 PACS / RIS 系统的无缝对接，确保报告流转合规可追溯。

5.3 质控管理功能要求

5.3.1 影像质量检测要求

为实现影像采集全流程质量管控，及时排查缺陷、规范技师操作，支撑科室质控闭环管理，本节提出具体要求：

a) 应支持自动识别影像采集过程中的常见质量问题，包括伪影、分辨率不足、体位不当、标识缺失等；
b) 应支持按缺陷严重程度（轻微、一般、严重）分级标记，针对可修正问题推送针对性重拍建议与操作指导，严重缺陷自动拦截并提醒技师处理；
c) 应支持生成影像质量检测统计报表（按科室、技师、设备、时间维度），支撑科室质控管理决策与持续改进。

5.3.2 诊断合规性质检要求

为保障诊断报告规范性、逻辑性与合规性，规避诊疗风险，实现AI辅助质控与人工复核结合，本节提出具体要求：

a) 应支持基于循证医学知识库与医疗规范，对诊断结论、用药建议、检查建议的规范性进行 AI 审核，拦截不合理诊断与超说明书用药相关影像支持依据；
b) 应支持自动检查诊断报告的完整性（如是否遗漏关键描述、签名是否完整）、逻辑性（如影像表现与诊断结论是否矛盾），标记缺失项及矛盾表述并提醒修改；
c) 应支持质控规则自定义与模型更新，适配不同地区、不同级别医院的质控要求。

5.4 科研与协同要求

5.4.1 真实世界研究支持要求

为赋能医学科研数字化转型，提供高效数据分析工具与数据支撑，简化科研流程，本节提出具体要求：

a) 应支持提供影像数据与临床数据（电子病历、检验结果、随访数据）的关联分析工具，支持疾病亚型分类、治疗效果相关性挖掘、预后因素筛选等研究场景；
b) 应支持兼容 CSV、JSON、DICOM 等常见科研数据格式，支持与科研管理系统无缝对接，实现研究数据的导入/导出与共享管理。

5.4.2 区域协同建模要求

为打破机构数据壁垒，实现多中心数据协同建模与模型共享，兼顾数据隐私与模型性能提升，本节提出具体要求：

a) 应支持跨机构共建专科疾病大模型（如肺癌、脑卒中、乳腺疾病等），基于联邦学习技术实现多中心数据“可用不可见”，保护数据隐私的同时提升模型性能；
b) 应支持提供多中心数据协同训练工具，支持数据标准化对齐、分布式训练任务调度、训练过程监控与模型性能评估，打破单一机构数据量级限制；
c) 应支持模型训练成果跨机构共享与适配优化，允许合作机构基于核心模型进行本地化微调，满足个性化临床需求。

5.4.3 规培演练环境要求

为搭建专业化医学影像规培体系，模拟临床场景提升医师实操能力，实现规培过程量化评估，本节提出具体要求：

a) 搭建虚拟病人影像演练系统，模拟各类常见病、疑难病、急危重症的影像处置场景，提供病例库分类管理（按病种、难度等级）；
b) 提供病例难度分级（初级、中级、高级）与个性化训练方案定制，支持训练过程记录与效果评估（如诊断准确率）；
c) 内置专家点评与知识点解析模块，针对训练过程中的错误诊断提供原因分析与权威解读，辅助年轻医师快速提升影像解读能力。

5.5 知识持续更新功能要求

5.5.1 知识图谱整合要求

为整合权威、动态的医学影像知识体系，支撑模型智能推理与临床辅助决策，保障知识准确性与时效性，本节提出具体要求：

a) 支持整合权威医学教材、最新临床指南、专家共识、高质量期刊文献及征象－诊断关联规则，更新影像－诊断知识图谱；
b) 支持知识图谱交互式查询，医生可通过图谱查看疾病与影像征象、临床症状的关联关系，辅助理解诊断逻辑；
c) 建立知识更新审核机制，新增知识需经医疗 AI 专家委员会审核通过后方可入库，确保其医学准确性、权威性与时效性。

5.5.2 增量学习机制要求

为实现模型持续迭代优化，在保留原有知识的基础上快速融入新数据、新知识，避免知识遗忘，本节提出具体要求：

a) 应支持高效参数更新，可高效融入新疾病知识、新增病例数据及专家标注反馈，实现模型能力的持续迭代；
b) 应支持具备旧知识保护机制，通过正则化、对比学习等技术，避免增量训练过程中出现知识遗忘（灾难性遗忘），保障原有诊断能力不下降；
c) 应支持按专科、疾病类型开展定向增量训练，提升模型在特定领域的精准度，训练过程可监控、可回溯，训练结果可评估。

5.5.3 个性化知识推送要求

为精准匹配医师专业提升需求，定向推送前沿知识与培训内容，助力医师能力持续进阶，本节提出具体要求：

a) 应支持基于医生疑难病例处理结果，定向推送相关继续教育课程、最新临床指南及专家共识；
b) 应支持医生自定义关注领域（如专科病种、新技术），推送该领域的知识更新、学术进展及典型病例，助力医生持续提升专业能力。

6 数据交互接口要求

6.1 接口设计要求

为保障接口通用性、兼容性与安全性，实现系统间高效互联互通，降低集成改造成本，本节针对接口设计提出总体要求：

a) 标准化原则：应支持 RESTful API 设计规范，采用 JSON / DICOM 等标准化数据交换格式与统一接口命名规则，确保接口通用性与互操作性；
b) 兼容性原则：应支持兼容 HL7 FHIR 等主流医疗系统接口规范，支持接口版本向下兼容，降低现有系统集成改造成本；
c) 安全性原则：应支持所有接口均需通过身份认证、权限校验与数据加密传输，严格防范未授权访问与数据泄露；
d) 可扩展性原则：应支持接口设计预留扩展字段与版本升级路径，支持新增功能与场景扩展，满足未来业务发展需求；
e) 易用性原则：应支持提供含调用示例、参数说明、错误码解释的清晰接口文档，支持批量操作与异步处理，并配备接口调试工具，降低开发接入难度；
f) 可靠性原则：应支持接口具备幂等性设计（重复调用不产生异常结果），支持请求重试与响应结果校验机制，确保数据传输完整性与一致性。

6.2 接口传输要求

6.2.1 传输协议与格式要求

为规范接口传输流程，保障数据传输稳定、规范、无乱码，实现高效数据交互，本节提出具体要求：

a) 通信协议：应支持采用 HTTPS 1.3 协议进行数据传输，确保传输过程安全加密；

b) 数据格式：应支持请求与响应数据优先采用 JSON 格式，影像数据支持 DICOM 格式二进制传输（含压缩与解压功能）；
c) 字符编码：应支持统一采用 UTF－8 编码，避免字符解析乱码问题；
d) 错误处理：应支持接口需返回标准化错误码、错误信息及解决方案建议，便于问题排查。

6.2.2 加密与认证要求

为防范接口传输过程中的数据泄露、篡改与非法访问，保障数据传输全流程安全，本节提出具体要求：

a) 身份认证：应支持采用 OAuth 2.0 认证机制，支持 API 密钥、令牌（Token）、数字证书等多种认证方式，令牌有效期可配置；
b) 数据加密：应支持传输数据采用 AES－256 加密算法处理，敏感字段（如患者标识信息）额外进行脱敏与二次加密；
c) 签名验证：应支持支持采用 SHA－256 算法的请求参数签名验证，防止请求被篡改或伪造，确保请求来源合法性。

6.2.3 传输性能要求

为保障接口高并发、高吞吐、低延迟传输，满足临床高频调用需求，本节针对传输性能提出具体要求：

a) 影像传输速度：应支持断点续传与分片传输，单幅 1024×1024 像素高清影像传输时间≤3 秒，批量影像传输速度可线性扩展；
b) 并发处理能力：应支持日均超 5 万次接口调用，峰值并发请求处理能力≥200QPS，接口调用成功率≥99.9%；
c) 流量控制：应支持接口流量监控与限流机制，可根据用户需求配置限流阈值，避免系统过载。

6.3 接口改造要求

6.3.1 院内关联系统接口改造要求

a) PACS 系统接口
   1) 改造内容：应支持新增支持主动推送与被动拉取的影像数据推送接口，实现检查完成的影像数据向大模型平台的自动同步；新增模型诊断结果回写接口，将诊断建议与结构化报告回写至 PACS 系统；
   2) 数据需求：应支持需推送 DICOM 格式影像文件、脱敏后的患者基本信息、检查部位、检查目的、检查时间、设备信息等关键数据；
   3) 交互方式：应支持同步调用与异步回调两种模式，异步回调需提供结果确认机制，确保数据传输可靠性；
   4) 适配要求：应支持兼容 GE Cen 等主流 PACS 系统的接口规范，并提供适配测试报告。
b) HIS/LIS 系统接口
   1) 改造内容：应支持新增患者基本信息查询接口、临床诊断信息查询接口、检验结果数据查询接口、医嘱信息查询接口；新增诊断相关数据统计接口，支持向 HIS 系统推送诊疗质量统计数据；
   2) 权限控制：应支持接口访问需严格遵循医院数据权限管理规范，采用角色授权机制，仅开放必要数据字段，禁止访问与诊疗无关的敏感信息；
   3) 数据同步：应支持实时查询（如诊疗过程中）与定时同步（如夜间批量同步）两种模式，定时同步频率可配置，满足不同场景的数据需求；
   4) 格式要求：应支持返回数据需符合 HL7 FHIR 标准化编码规范，支持通过患者唯一标识与影像数据进行关联匹配。
c) 门诊/住院工作站接口
   1) 改造内容：应支持新增大模型诊断结果嵌入接口，支持在工作站界面内直接展示诊断建议、病灶标注与结构化报告；新增一键调用模型服务接口，支持医生在工作站内发起影像分析请求；

2) 交互体验：应支持诊断结果实时回显，操作流程无缝融入医生现有工作流，不影响原有诊疗节奏，界面响应延迟≤300ms；
3) 操作权限：应支持按医生职称、科室、岗位设置接口访问权限，支持权限精细化管控（如仅允许放射科医师编辑报告），确保功能使用合规；
4) 反馈机制：应支持医生对诊断结果进行评价（如认可、修正、否定）与反馈（填写意见），反馈数据自动同步至模型训练平台，用于模型优化。

6.3.2 院外关联系统接口改造

a) 区域健康信息平台接口
1) 改造内容：应支持新增跨机构影像数据查询接口（支持按患者唯一标识跨机构检索）、诊断结果共享接口、质控数据上报接口。
2) 数据规范：应支持严格遵循区域医疗数据交换标准，支持患者唯一标识（如医保电子凭证号）跨机构映射，确保数据一致性与关联性。
3) 权限管理：应支持基于区域医疗协同授权机制，实现跨机构接口访问权限动态管控，仅允许授权机构访问相关数据。
4) 同步机制：应支持诊断结果实时推送（如远程会诊场景）与历史数据追溯查询，支撑区域质控管理与医疗服务效率评估。

b) 生态合作伙伴系统接口
1) 改造内容：应支持开放标准化 API 接口与微服务组件，包括模型调用接口、数据上传 / 下载接口、结果回调接口、知识图谱查询接口等。
2) 接口类型：应支持提供 RESTful API 与 SDK 两种接入方式，支持 Python、Java、C＋＋等多种编程语言调用。
3) 接入流程：应支持提供标准化接入流程（申请－审核－测试－上线）与审核机制，对合作伙伴进行资质审核，确保合规接入。
4) 版本管理：应支持建立接口版本控制机制，支持版本查询、升级提醒与平滑过渡，旧版本接口保留至少 6 个月的过渡期，保障合作伙伴系统稳定。

c) 监管平台接口
1) 改造内容：应支持新增模型运行日志上报接口、诊断数据统计上报接口、合规性检测结果上报接口、故障告警上报接口。
2) 数据要求：应支持按国家药品监督管理局、卫生健康委员会等监管部门要求，上报模型基本信息、运行状态、诊断准确率、不良事件等相关数据，确保数据真实、完整、可追溯。
3) 上报频率：应支持实时上报（如故障告警、不良事件）与定时汇总上报（如每日 / 每月统计数据）两种模式，上报频率可按监管要求配置。
4) 安全要求：应支持采用加密传输与签名验证机制，确保上报数据不被篡改，上报日志留存时间≥1 年，支持监管部门追溯核查。

7 性能要求

7.1 处理效率指标

为保障模型临床响应速度，满足诊疗实时性需求，提升批量数据处理效率，本节针对处理效率提出量化指标：

a) 应支持单模态影像诊断响应时间≤45 秒（从影像数据输入完成到诊断结果输出，含预处理与推理）；
b) 应支持多模态数据融合诊断响应时间≤10 秒（含 2 种及以上模态影像、文本等多元数据的协同处理与推理）；
c) 应支持结构化报告生成时间≤5 秒；

7.2 并发处理能力

为保障模型高并发场景下稳定运行，兼顾诊断精度与训练效率，满足大规模临床应用需求，本节提出具体要求：

a) 应支持日均支持超 5 万次高并发推理请求，峰值并发请求处理能力≥200QPS，并发处理过程中系统无卡顿、无数据丢失；
b) 应支持分钟级扩容千卡级 GPU 集群，可应对突发公共卫生事件期间访问量暴增（预计峰值为日常 3 倍以上），扩容过程不影响系统正常运行；

7.3 应支持多用户同时在线操作时，系统响应时间无明显延迟（延迟增加≤500ms），支持≥500 名用户同时在线使用（含诊断、报告编辑、数据查询等操作）；功能指标

a) 辅助诊断指标：
   1） 应支持常见疾病辅助诊断（如肺炎、骨折、脑出血、肺结核、脂肪肝等）≥200 种，诊断结果专业医生验证通过率≥90%；
   2） 应支持疑难疾病辅助诊断（如早期肺癌、胰腺癌、罕见神经系统疾病等）≥30 种，诊断结果专业医生验证通过率≥80%；
   3） 应支持报告术语标准化准确率≥99%。
b) 训练功能指标：
   1） 专科疾病增量训练：单次新增数据量≤10 万幅影像时，应支持增量训练更新周期≤24 小时；
   2） 模型微调效率：应支持生态伙伴基于自有数据进行微调，1 万幅影像数据的微调周期≤12 小时。

7.3 系统可用性指标

为保障系统长期稳定运行、降低故障停机风险，提升用户操作体验，满足临床不间断服务需求，本节提出具体要求：

a) 应支持系统全年可用性≥99.9%，每月计划外停机时间不超过 43.2 分钟（按 30 天/月计算），计划内维护需提前 72 小时通知用户；
b) 应支持故障恢复时间≤30 分钟（从故障发生到系统恢复正常运行），支持故障自动告警与故障原因初步诊断；
c) 应支持离线缓存功能，网络中断时核心诊断功能（如已缓存影像的分析、报告编辑）可维持 2 小时以上正常使用，网络恢复后自动同步数据；
d) 应支持用户操作成功率≥99.5%，界面加载时间≤2 秒，操作响应时间≤500ms（不含模型推理时间）。

8 安全要求

8.1 安全应用环境要求

为构建安全可控的应用环境，规范权限管理、操作行为与漏洞防护，防范内部与外部安全风险，本节提出具体要求：

a) 权限管理：应支持采用基于角色的访问控制（RBAC）机制，结合最小权限原则与数据分级分类管理要求，为不同用户角色分配精准的操作权限；
b) 应支持细粒度权限控制，可按科室、功能模块、数据范围（如特定病种数据、特定患者数据）、操作类型（查询、编辑、删除、导出）设置访问权限；
c) 应支持实现操作权限动态调整与权限变更审计，权限变更需经过审批流程，变更记录留存时间不低于 1 年，确保权限管理可追溯；
d) 应支持多因素认证（如密码＋动态令牌、密码＋生物识别），针对报告审核、数据导出、系统配置等核心操作强制启用多因素认证；
e) 应支持建立密码安全管理规范，要求密码具备复杂度（包含大小写字母、数字、特殊符号）、定期更换（最长周期 90 天）、禁用最近 5 次历史密码；
f) 应支持内置应用防火墙与入侵防御模块，有效防御 SQL 注入、XSS 跨站脚本、CSRF 跨站请求伪造、命令注入等常见网络攻击；

g) 应支持定期开展应用漏洞扫描（每月至少 1 次）与渗透测试（每季度至少 1 次），发现漏洞后的修复响应时间不超过 24 小时，高危漏洞修复时间不超过 8 小时；
h) 应支持实现敏感操作日志记录与审计，涵盖用户登录/注销、数据查询/导出/修改/删除、诊断结果修改、系统配置变更等关键操作，日志内容需包含操作人、操作时间、操作内容、操作 IP、操作结果，且日志留存时间不低于 1 年；
i) 应支持建立应用程序异常监控机制，对异地登录、多次密码错误等异常登录行为，批量导出数据、高频次修改报告等异常操作，以及系统异常运行状态进行实时告警，告警响应时间不超过 5 分钟；支持应用程序安全补丁自动更新与手动更新两种模式，补丁更新前需开展兼容性测试，避免影响系统正常运行。

8.2 安全通信网络要求

为保障网络通信安全，实现网络分区管控、传输加密与攻击防护，杜绝数据传输泄密与非法入侵，本节提出具体要求：

a) 网络分区：应支持按功能划分为数据采集区、模型训练区、推理服务区、管理区、DMZ 区，各区域间实现逻辑隔离，通过防火墙、ACL 策略控制区域间数据流向；
b) 传输加密：应支持所有网络传输数据采用 TLS 1.3 协议加密，患者隐私信息、诊断报告等敏感数据额外采用端到端加密，确保传输过程中数据不被窃取、篡改；访问控制：部署下一代防火墙（NGFW），基于 IP 地址、端口、协议、应用类型、用户角色等多维度设置访问控制策略，禁止非法访问核心业务系统；
c) 流量监控：应支持实时监控网络流量，对大流量下载、高频次访问、异常端口通信等异常流量进行识别、告警与阻断，支持流量日志留存不低于 6 个月；
d) 边界防护：应支持禁止核心业务系统直接接入互联网，远程维护与访问需通过企业级 VPN（支持加密传输与身份认证），且 VPN 接入需经过多因素认证；
e) 抗 DDoS 攻击：应支持部署抗 DDoS 攻击防护设备，支持对 SYN Flood、UDP Flood、ICMP Flood 等常见 DDoS 攻击的识别与防御，保障系统在攻击场景下正常运行。

8.3 安全区域边界需求

为强化核心区域边界防护，规范跨区域访问与数据摆渡，防范边界渗透风险，保障核心业务安全，本节提出具体要求：

a) 防火墙配置：应支持在模型训练区、推理服务区等核心区域边界部署下一代防火墙，实现数据包过滤、状态检测、应用层过滤、VPN 接入控制等功能，防火墙规则每季度至少开展 1 次定期审计；
b) 入侵检测 / 防御：应支持在核心区域边界部署入侵检测系统（IDS）与入侵防御系统（IPS），实时监测并阻断端口扫描、暴力破解、恶意代码传播等恶意攻击行为，告警响应时间不超过 5 分钟；
c) VPN 接入：应支持远程维护与访问需通过企业级 VPN，支持多因素身份认证、AES－256 加密传输与访问权限控制，VPN 登录日志留存不低于 1 年；
d) 安全审计：应支持对区域边界的所有访问行为进行日志记录与审计，包括接入 IP、访问时间、访问内容、操作结果等，日志留存时间不低于 6 个月，支持按多维度查询与分析；
e) 数据摆渡：应支持跨区域数据传输需通过专用数据摆渡机、光盘摆渡等安全摆渡设备，禁止直接拷贝，确保数据传输可追溯，摆渡数据需经过病毒查杀与安全检测；
f) 边界隔离：应支持核心业务区域与非核心区域、内部网络与外部网络之间实现严格的边界隔离，禁止未经授权的跨区域数据流动。

8.4 安全容灾备份要求

a) 数据备份
   1) 采用“3－2－1”备份策略：应支持至少保留 3 份数据副本，存储在硬盘、磁带等 2 种不同介质上，其中 1 份存储在距离生产中心不低于 100 公里的异地；备份频率：核心业务数据（如诊断结果、患者影像、操作日志）实时备份；非核心数据（如统计报表、历史训练数据）执行每日增量备份与每周全量备份。

2) 备份验证：应支持每月至少开展 1 次备份数据恢复测试，验证备份数据的完整性与可用性，测试结果需形成报告留存。
3) 备份存储：应支持备份数据应存储于安全级别不低于生产环境的存储设备，采用 AES－256 加密技术进行加密存储；访问备份数据需通过严格的身份认证与权限校验流程。
4) 备份管理：应支持建立备份数据生命周期管理机制，依据数据重要性设定备份保留期限——核心数据保留期≥3 年，非核心数据保留期≥1 年；到期数据自动清理，且清理过程需可追溯。

b) 容灾恢复
1) 应支持建立异地容灾中心，与生产中心的距离≥100 公里；核心数据采用同步复制技术，非核心数据采用异步复制技术，确保灾备中心与生产中心的数据一致性。
2) 应支持制定详细的容灾恢复预案，明确灾备切换的触发条件、切换流程、责任人、操作步骤及恢复目标，预案需经过评审与备案。
3) 容灾恢复目标：应支持总体 RTO（恢复时间目标）≤4 小时，RPO（恢复点目标）≤15 分钟；针对核心诊断功能，RTO≤2 小时，RPO≤5 分钟。
4) 容灾演练：应支持定期开展容灾演练，每年至少 2 次（含完整切换演练与部分功能演练）；演练后需进行总结评估，优化容灾恢复流程。
5) 故障应对：应支持建立故障分级机制（分为一般、较大、重大、特别重大四级），针对不同级别故障制定相应的应急响应流程，确保故障得到快速处置与系统恢复。

8.5 安全管理体系需求

a) 制度建设
1) 应支持建立完善的信息安全管理制度体系，包含数据安全管理办法、权限管理规范、应急响应预案、安全审计管理办法、备份与恢复管理规范等；
2) 应支持制定医疗数据分级分类标准，将数据划分为核心数据（如患者隐私信息、诊断报告）、重要数据（如影像数据、训练数据）、一般数据（如统计报表），明确不同级别数据在存储、传输、使用、销毁环节的安全要求；
3) 应支持建立安全事件报告与处置流程，明确安全事件的发现、上报、研判、处置、总结等环节的要求，确保安全事件及时发现、快速响应、有效处置；
4) 应支持定期对安全管理制度进行评审与更新（每年至少 1 次），确保制度适配业务发展与政策变化。

b) 人员管理
1) 应支持对系统相关人员（研发、测试、运维、医疗专家）开展全面的安全培训与考核，培训内容涵盖安全管理制度、数据隐私保护要求、安全操作规范、应急处置流程等，考核合格后方可上岗；
2) 应支持建立人员离岗离职安全管理流程，及时收回访问权限、销毁敏感资料（如纸质文档、存储介质）、删除系统账号，开展离岗安全谈话并签订保密承诺书；
3) 应支持与所有接触敏感数据的人员签订保密协议，明确人员安全责任与义务，防范内部人员数据泄露、滥用或恶意操作；
4) 应支持建立人员安全考核机制，将安全工作表现纳入绩效考核，对违反安全管理制度的行为进行追责。

c) 审计与合规
1) 应支持建立全面的安全审计体系，对数据全生命周期操作（采集、存储、传输、使用、销毁）、系统运行状态、用户行为等进行全面日志记录与审计；
2) 应支持审计日志留存时间≥1 年，支持按时间、用户、操作类型、数据类型等多维度查询与分析，具备日志导出与报表生成功能；
3) 应支持定期开展安全合规性评估（每半年至少 1 次），确保符合《数据安全法》《个人信息保护法》《医疗器械监督管理条例》等相关法规要求，评估结果形成报告留存；
4) 应支持配合监管部门检查，提供必要的审计日志、合规性证明材料、安全管理制度等，积极落实监管要求；

5) 应支持建立合规性预警机制，关注医疗行业法规标准变化，及时调整安全管理策略与制度，确保持续合规。