ICS

T/GXDSL

团　　体　　标　　准

T/GXDSL —2026

AI+临床辅助检查管理规范

AI+ Clinical Auxiliary Examination Management Specification

（工作组讨论稿）

（本草案完成时间：2026 - 5 - 6 ）

2026 - - 发布　　2026 - - 实施

广西电子商务企业联合会　发布

目　　次

前　言

本文件依据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。

本文件由广西产学研科学研究院提出。

本文件由广西电子商务企业联合会归口。

本文件起草单位：

本文件主要起草人：

本文件为首次发布。

AI+临床辅助检查管理规范

1 引言

为深入贯彻落实国务院《关于深入实施“人工智能+”行动的意见》（国发〔2025〕11 号）及国家卫生健康委《关于促进和规范“人工智能+医疗卫生”应用发展的实施意见》（国卫办规划发〔2025〕30 号）核心精神，主动顺应人工智能技术与临床辅助检查领域深度融合的发展趋势，破解当前 AI 辅助诊断应用中存在的准确率波动、数据集偏倚、责任追溯不畅、数据安全隐患等突出问题，筑牢医疗质量安全底线，特制定本文件。本文件立足国家“人工智能+医疗卫生”高质量发展战略定位，构建 AI 介入临床辅助检查全流程、全要素管理体系，明确管理基准与技术要求，坚守“赋能不替代、辅助不决策”的核心原则，推动 AI 技术在临床辅助检查领域规范、安全、高效应用，助力医疗服务提质增效，更好满足人民群众日益增长的健康服务需求，为健康中国建设注入科技动能。

2 范围

明确了各级各类医疗机构应用人工智能技术开展临床辅助检查（涵盖医学影像、电生理、实验室检验及病理检查等重点领域）的技术准入、数据治理、临床应用、质量控制、安全保障及责任落实等全流程要求，是规范 AI 技术在临床辅助检查领域应用的基础性、指导性文件。适用于全国各级各类利用 AI 软件（含嵌入式 AI 设备、独立医用软件及大模型决策支持系统）开展临床辅助检查的医疗卫生机构，覆盖 AI 技术应用、管理、维护全环节。同时适用于参与 AI 辅助检查相关产品研制、生产、售后的各类企业，包括广西产学研科学研究院及全国相关人工智能医疗器械研发、生产单位，推动产学研协同规范发展，助力构建全国统一的 AI 医疗应用标准体系。

3 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，确保本规范与国家最新标准、政策保持一致，彰显规范性与权威性。

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 39725-2020 信息安全技术健康医疗数据安全指南

GB/T 41813.1-2022 信息技术智能语音交互测试方法

YY/T 1833.1-2022 人工智能医疗器械质量要求和评价 第 1 部分：术语

YY/T 1833.4-2025 人工智能医疗器械质量要求和评价 第 4 部分：可追溯性

YY/T 1858-2023 人工智能医学影像辅助诊断系统临床评价方法

《医疗器械生产质量管理规范》（2025 年修订版，国家药监局，2026 年 11 月 1 日施行）

4 术语和定义

YY/T 1833.1-2022 界定的以及下列术语和定义适用于本文件，统一行业认知，避免执行偏差，为规范落地提供清晰的概念支撑。

4.1 AI+临床辅助检查

指应用机器学习、深度学习或大语言模型等人工智能核心技术，对人体样本（血液、体液、组织等）或生理信号（影像、心电等）进行自动识别、精准测量、科学标注、分类研判或图像重建的标准化过程，是提升临床检查效率、优化诊疗流程的重要技术手段。

4.2 人工智能医疗器械

指基于人工智能技术研发、具备明确医疗器械预期用途的独立软件或嵌入式软件，其核心处理对象为临床医疗数据。依据国家药品监督管理局分类界定标准，辅助筛查类产品通常为二类医疗器械，可提供初步筛查提示；辅助诊断类产品（能给出明确倾向性诊断结论）为三类医疗器械，需严格遵循更高标准的准入与监管要求，确保临床应用安全有效。

4.3 人机协同复核机制

指 AI 系统完成分析并输出结果后，必须由具备相应执业资质的临床医师进行全面复核、确认或修正的强制性操作机制，明确 AI 输出结果仅作为临床辅助参考，不得直接作为最终诊断报告发布，坚守医师为诊疗决策主体的核心原则，防范医疗风险。

5 缩略语

AI：人工智能（Artificial Intelligence）

DICOM：医学数字成像和通信标准（Digital Imaging and Communications in Medicine）

HL7：卫生信息交换标准（Health Level Seven）

AUC：曲线下面积（Area Under Curve），用于评估 AI 诊断模型的准确性

DIC：数据完整性校验（Data Integrity Check），保障医疗数据真实、完整、可追溯

6 技术准入与设备管理

6.1 资质要求

6.1.1 严格落实国家医疗器械监管要求，应用于临床辅助诊断的 AI 系统，必须持有国家药品监督管理局核发的三类医疗器械注册证；用于纯筛查、流程优化（不涉及诊断结论输出）的 AI 系统，至少持有一类或二类医疗器械注册证，严禁无资质、超资质应用，筑牢技术准入安全防线。

6.1.2 研制企业（包括但不限于广西产学研科学研究院合作的研发机构）应提供完整、规范的技术白皮书，明确训练集、调优集、验证集的具体构成（含样本量、地域分布、设备型号、病例覆盖范围等），确保数据来源合法、合规、可追溯，严格符合《人工智能医疗器械 质量要求和评价 第 4 部分：可追溯性》（YY/T 1833.4-2025）及国家数据安全相关规定，助力构建高质量医疗数据集和可信数据空间。

6.2 更新迭代管理

6.2.1 建立 AI 算法分类更新管理机制，明确 AI 算法更新分为“微小更新”（如 Bug 修复、界面优化，不影响核心决策逻辑）和“重大更新”（如重新训练模型、扩大适应症范围、优化核心算法等），分类实施管理，兼顾创新迭代与安全可控。

6.2.2 发生重大更新时，医疗机构需重新开展临床准入评估，严格审核更新后模型的性能、安全性和适用性，并向本单位医学伦理委员会及设备管理委员会备案。更新后需保留旧版本至少 3 个月，用于新旧版本性能对比观察，防范新模型出现灾难性遗忘、性能衰减等问题，确保更新过程规范有序，保障临床应用连续性。

6.2.3 严格落实可追溯性要求，算法训练用数据集的时间戳、标注人员的资质信息（如标注医师的职称、工作年限、专业资质等）必须作为元数据与系统日志绑定存储，实现全流程可追溯，全面满足 YY/T 1833.4-2025 规定的可追溯性要求，同时契合人工智能科技伦理审查中关于数据规范的相关要求。

7 数据治理与质量控制

7.1 数据输入规范

7.1.1 影像类数据：必须严格符合 DICOM 3.0 标准，图像质量需通过 AI 系统内置质控模块及人工双重检测。例如，在 CT 肺结节筛查中，若图像噪声比超过预设阈值（如 SD>15）或扫描层厚>1.25mm，AI 系统应自动拒绝分析并明确提示“图像不符合质控标准”，技师需重新采集图像，确保输入数据质量，为 AI 精准分析提供基础。

7.1.2 检验类数据：接入 AI 系统的临床实验室数据，需严格符合《医疗机构 POCT 检验信息化应用技术规范》的接口要求，建立数据传输全流程校验机制，确保数据传输过程中不丢失、不改写、不泄露，保障数据的真实性、完整性和时效性。

7.1.3 数据脱敏：进入 AI 系统的所有医疗数据必须进行规范的去标识化处理，严格移除患者直接标识符（姓名、身份证号、住院号、联系方式等），仅保留必要的生物特征（年龄、性别、病史标签等），兼顾数据利用与隐私保护，严格遵循国家健康医疗数据安全相关规定，落实数据安全管理和个人信息保护负面清单要求。

7.2 数据偏见与失效管理

7.2.1 医疗机构应建立 AI 系统决策公平性监测机制，每季度对 AI 系统的决策分布进行统计学分析，重点关注不同亚组（如特定年龄段、特定民族、特定设备来源、特定地域患者）的诊断置信度差异。若发现某一亚组的诊断置信度显著低于平均水平（$p<0.05$），应立即暂停该亚组相关 AI 应用，及时上报研制企业进行偏见修正，同时向属地卫生健康行政部门备案，确保 AI 决策的公平性、包容性，契合人工智能科技伦理审查要求。

7.2.2 研制企业应建立“数据漂移”常态化监测机制，实时跟踪临床数据分布变化，当实际临床数据分布与模型训练集分布出现偏移（如新出现的病毒变异株导致影像特征改变、疾病谱变化等）且影响 AI 诊断准确率超过 2%时，系统应自动触发告警，及时通知医疗机构及相关管理部门，同步启动模型优化流程，确保 AI 系统适应临床实际需求，保障应用质量。

8 临床应用规范

8.1 人机协同操作流程

8.1.1 优先级与排序：AI 系统应对检测出的阳性结果或危急值进行分级风险标记，优先推送高风险病例。例如，心电图 AI 分析应在 1 分钟内给出初步分类（如“STEMI 阳性”），并立即提醒医师，医师必须在 10 分钟内完成复核确认，确保危急重症病例得到快速处置，提升急危重症抢救效率，契合国家临床诊疗质量安全相关要求。

8.1.2 假阴性/假阳性处理预案：针对不同临床场景明确 AI 性能阈值，在放射科肺结节检测场景下，AI 检出率应≥95%（即允许漏诊率<5%）。对于 AI 标记为“阴性”但医师肉眼发现可疑病灶，或 AI 标记为“阳性”但经复核确认无异常的案例，必须强制记录相关信息并上报至医疗机构不良事件数据库，同时反馈给研制企业，用于算法优化迭代，持续提升 AI 诊断准确性。

8.1.3 弃用机制：明确临床医师的主导权，医师有权一键关闭 AI 辅助视图。若医师判断 AI 输出结果无临床价值、存在误导或与临床实际不符，必须在系统中详细选择弃用原因（如“伪影干扰”“解剖变异”“算法局限性”等）。当某一 AI 系统的弃用率超过 10%时，需立即触发性能再评估流程，由医疗机构联合研制企业开展全面排查，必要时暂停系统应用，确保 AI 应用的实用性和可靠性。

8.2 危急值管理

8.2.1 AI 系统发现符合《国家医疗服务与质量安全报告》定义的危急值（如室性心动过速、气胸压缩>50%、颅内急性大出血等）时，立即触发最高优先级警报，同步推送至接诊医师、科室护士及相关管理人员，确保相关人员第一时间知晓。

8.2.2 建立危急值预警分级上报机制，AI 预警后，若在预设时间阈值内（如 30 分钟）未被医师签收确认，系统需自动升级上报至科室主任及医务科，由医务科督促相关医师及时处置，形成闭环管理，防范危急值漏报、延误处置等风险，保障患者生命安全。

9 质量评价与追溯

9.1 实时质控指标

医疗机构应建立 AI 辅助检查质量控制仪表盘，实时监控以下核心 KPI 指标，确保 AI 应用质量持续达标，助力医疗服务高质量发展：

9.1.1 准确率：AI 诊断结果与金标准（病理诊断或专家共识）的符合率，单一病种 AUC 应≥0.95，确保 AI 诊断的精准性；

9.1.2 处理速度：AI 完成分析的时间（从图像上传完成到结果生成），CT 影像应在 3 分钟内完成，心电图应在 30 秒内完成，提升临床检查效率，优化患者就医体验；

9.1.3 使用依从性：医师在 AI 提示危急值后采取干预措施的比率，确保危急值得到及时处置，保障医疗质量安全。

9.2 定期外审

9.2.1 建立 AI 系统定期外审机制，每年委托具备法定资质的第三方检测机构（如中国食品药品检定研究院或具备 CNAS 资质的实验室）对 AI 系统进行盲法测试，确保测试结果客观、公正，提升评价

权威性。

9.2.2 测试集构建需兼顾代表性与复杂性，必须包含至少 10%的罕见病例及 5%的干扰病例（如体内有金属植入物的影像、运动伪影图像、合并多种基础疾病的病例等），全面评估 AI 系统的鲁棒性和适用性，确保 AI 系统在复杂临床场景下仍能稳定发挥辅助作用。

9.3 可追溯性要求

依据 YY/T 1833.4-2025 及国家医疗质量安全追溯相关规定，每个 AI 辅助生成的检查报告必须关联完整的可追溯信息，实现“全程可查、责任可究”，具体包括：所使用的 AI 软件版本号及模型 MD5 校验值，确保模型可追溯；算法输出的特征图或热力图（如肺结节位置标记、病灶特征标注等），为医师复核提供依据；最终确认医师的电子签名及操作时间戳，明确诊疗责任；若 AI 拒绝分析（因数据质量、系统故障等问题），需详细记录拒绝的代码和具体原因，便于后续排查整改。

10 数据安全与隐私保护

10.1 网络安全

AI 系统若部署于院内局域网，应采取物理隔离或网闸逻辑隔离方式，与外网严格区分，防范网络攻击、数据泄露等风险；若涉及云端远程 AI 会诊，数据传输通道需严格符合《信息安全技术 健康医疗数据安全指南》（GB/T 39725-2020）要求，采用国密算法 SM4 进行加密传输，确保数据传输过程安全可控，落实国家健康医疗数据安全防护要求。

10.2 数据本地化与销毁

10.2.1 严格落实数据本地化存储要求，患者的原始检查数据（如 DICOM 文件、检验原始数据等）原则上应在医疗机构内部存储，严禁未经授权上传至研制企业的公有云训练库，坚守数据安全底线。

10.2.2 如确需将相关数据用于科研训练，需经过医院伦理委员会严格审批，签署规范的数据使用协议，明确数据使用范围、期限及责任，确保数据利用合法合规。数据保存期限严格依据《医疗机构病历管理规定》执行，门（急）诊病历由医疗机构保管，保存时间自患者最后一次就诊之日起不少于 15 年，保障数据可追溯性的同时，维护患者合法权益。

10.2.3 严格规范研制企业数据使用行为，研制企业不得以“优化算法”“技术升级”等名义，未经医疗机构二次授权擅自挪用、采集临床实时数据，严禁数据非法交易、泄露，落实数据安全管理负面清单要求，推动医疗数据安全有序流动。

11 应急管理

11.1 系统故障预案

建立 AI 系统故障应急处置机制，当 AI 系统出现服务中断（如 GPU 服务器宕机、API 接口超时、软件崩溃等）时，系统应在 5 秒内自动切换至纯人工模式（Failsafe 模式），确保临床检查工作不中断。故障期间，工作站显示的图像应为原始未处理图像，不得出现加载失败、乱码等情况影响医师阅片和诊疗决策，保障临床工作连续性。

11.2 算法回滚机制

建立 AI 算法应急回滚机制，当新版本 AI 系统导致大规模误报（例如 24 小时内误报率上升超过 5%）或出现严重性能问题时，医疗机构信息科应具备一键回滚至前一稳定版本的能力，回滚操作需在 10 分钟内完成，并详细保留操作日志，包括回滚原因、操作时间、操作人员等信息，便于后续追溯和问题排查，同时及时通知研制企业开展问题整改。

12 人员培训与资质

12.1 医师培训

使用 AI 系统的临床医师（如影像科医师、心内科医师、检验科医师等）必须完成至少 8 学时的岗前规范化培训，考核合格后方可开展 AI 辅助检查相关工作。培训内容重点包括： AI 的基本原理、核心算法及置信度解读方法，提升医师对 AI 结果的理解和判断能力；典型的 AI 故障模式（如对抗性攻击、遮挡失效、数据偏见导致的误判等）及应对方法，增强医师风险防范意识；相关法律法规、伦理规范及责任界定，明确医师对最终诊断报告负全部责任，坚守医疗伦理底线，契合人工智能科技伦理审查要求。

12.2 技师培训

操作扫描、检验等设备的技师需接受针对性培训，重点掌握如何根据 AI 系统的实时反馈调整设备参数，确保采集的数据符合 AI 分析要求。例如，在超声检查中，当 AI 提示切面不合格、数据采集不规范时，技师应及时调整探头角度、扫描参数，直至 AI 系统确认数据合格，保障输入数据质量，为 AI 精准分析奠定基础。同时，加强技师数据安全和隐私保护培训，规范操作流程。

13 研制企业责任

13.1 售后与不良事件监测

研制企业（包括提出单位广西产学研科学研究院及相关合作方）应建立健全全国统一的售后保障体

系和不良事件监测系统，主动向医疗机构明确告知 AI 系统的算法局限性（例如：“该算法对 3mm 以下的磨玻璃结节敏感度较低”“对罕见病诊断准确率有限”等），设置明确的警示标识，防范临床误用风险。企业应建立快速响应机制，对医疗机构报告的 AI 相关严重不良事件（如因 AI 漏诊、误判导致的医疗纠纷、患者伤害等），需在 48 小时内完成响应、排查，及时提出整改方案并落地实施，同时按规定向国家药品监督管理局及属地卫生健康行政部门上报，形成不良事件处置闭环，助力提升 AI 产品质量安全水平。

13.2 透明度报告

研制企业应坚持公开、透明的原则，每年向社会、医疗机构及相关监管部门公布 AI 系统的算法更新日志、真实世界性能报告（基于多中心、大样本临床数据），不得隐瞒 AI 系统的性能衰减、算法缺陷等负面数据。主动接受社会监督和行业监管，推动 AI 医疗产品持续优化升级，助力构建具有全球竞争力的 AI 医疗创新生态，服务国家“人工智能+”战略发展需求。