稳健医疗用品股份有限公司

（股票代码：300888.SZ）

负责任的人工智能管理制度

第一章 总则

第一条 稳健医疗用品股份有限公司（以下简称”公司”） 深知人工智能技术应用对用户权益、数据安全和社会责任的重要影响。为规范公司对人工智能应用的采购、部署和使用，促进人工智能技术安全、可靠、公平、透明和可持续地服务于生产经营，保护国家安全、社会公共利益以及个人和组织的合法权益，公司依据业务所在地适用的法律法规，并参考 ISO/IEC 42001 人工智能管理体系等相关标准，结合公司实际，制定本制度。

第二条 本制度适用于公司及纳入公司管理范围的分公司及子公司，并约束所有员工及代表公司行事的相关方。公司要求供应商及合作伙伴在合同约定下，承担相应责任。本制度确立的原则同样适用于公司开展的投资、并购等活动中涉及的人工智能事项。

第三条 现阶段公司主要作为第三方人工智能产品或服务的采购者、部署者和使用者，不自主研发、训练或对外运营基础模型、大模型。公司开展定制开发、微调、检索增强、智能体编排或以公司名义向外部主体提供人工智能功能时，应当根据活动性质承担相应责任，并适用不低于本制度规定的管理要求。

第四条 本制度所称：

1. **人工智能应用**，是指基于机器学习、深度学习、生成式人工智能等技术，能够对输入信息进行分析、推理、预测、推荐、决策或生成内容的系统、产品、功能或服务。

2. **人工智能生成合成内容**，是指利用人工智能技术生成或合成的文本、图片、音频、视频、虚拟场景等信息。

3. **自动化决策**，是指通过计算机程序自动分析、评估个人的行为习惯、兴趣爱好或者经济、健康、信用状况等，并据此作出决定的活动。

4. **人工智能影响评估**，是指在人工智能应用投入使用前或发生重大变更时，对其合法性、正当性、必要性以及对个人、组织、社会和环境可能产生的影响进行识别、分析、评价和处置的过程。

5. **受影响主体**，是指其权益可能受到人工智能应用的输入、输出、推荐、预测或决

策影响的个人或组织。

第二章 管理原则

第五条 公司使用人工智能应当遵守适用的法律法规、监管要求、商业道德和社会公德，具有明确、合理的业务目的，不得利用人工智能从事违法违规活动或损害国家安全、社会公共利益及他人合法权益。

第六条 公司应当尊重人的尊严、自主权和基本权利，合理设置人工监督、复核、干预、暂停和退出机制。人工智能应当辅助人员履行职责，不得以技术手段规避管理责任。

第七条 公司应当采取合理措施识别、预防和纠正可能造成不合理差别待遇的算法偏差，不得基于民族、种族、性别、年龄、宗教信仰、残障、健康状况、地域等因素实施违法或不合理的歧视。公司应当结合应用场景、受影响主体和风险等级，采取适当措施提升训练、测试和使用数据的相关性、准确性、完整性和代表性，定期开展偏差识别、公平性评估或必要的专项审查，并根据发现的问题及时采取纠正、缓释和优化措施。

第八条 公司应当根据人工智能应用的用途、风险和受影响程度，以清晰、易于理解的方式说明人工智能的使用情况、主要目的和重要局限。对可能对个人权益产生重大影响的结果，应当提供适当解释、人工复核和申诉渠道。在用户直接与人工智能系统交互、接收人工智能生成内容或接受人工智能辅助服务的场景中，公司应当以适当方式明确告知相关主体其正在与人工智能系统而非自然人交互，或者相关内容、建议、结论系由人工智能生成或辅助生成，但法律法规另有规定或者基于安全需要不宜披露的除外。对外提供的人工智能生成内容，应根据场景需要采取内容标识、水印、来源说明或其他合理方式，降低误认、误导和不当传播风险。

第九条 公司处理数据应当遵循合法、正当、必要、诚信和最小化原则，采取与数据敏感程度相适应的安全措施，不得超出授权范围收集、输入、使用、留存、共享或公开数据。

第十条 公司应当在人工智能应用的全生命周期开展风险管理，合理验证其准确性、稳健性、网络安全、数据安全和业务连续性，防止错误输出、提示词攻击、越权访问、数据泄露、模型操纵和其他滥用风险。

第十一条 公司建立职责明确、记录完整、结果可审计的人工智能治理机制。任何部门或人员不得以人工智能由第三方提供、结果由系统自动生成或技术机制复杂为由，免除其应承担的管理、审核和使用责任。

第十二条 公司在控制风险的前提下鼓励负责任的技术创新，综合考虑人工智能应用带来的经济、社会和环境影响，提升算力和能源使用效率，优先选择与业务需求相匹配、资源消耗合理的解决方案。公司在采购、开发、部署和使用人工智能应用及相关算力、模型、平台和数据中心资源时，应当综合考虑能源消耗、碳排放、水资源使用效率等环境因素，优先选择能效较高、环境足迹较低的技术方案和服务提供商，鼓励采用绿色数据中心、节能优化技术和可再生能源支持的基础设施。

第三章 治理架构与职责

第十三条 公司建立‘决策层、管理层、执行层’相互衔接的人工智能治理架构，并明确各层级职责。公司已组建由高级管理层、合规、技术、业务等相关部门负责人组成的专业治理机构，负责统筹协调、风险决策和监督。根据事项需要，可引入内外部专家参与评估。

第十四条 公司人工智能治理决策机构负责审议人工智能管理方针、目标和重大制度，审议高风险或具有重大影响的人工智能应用，协调重大资源投入，并监督重大风险处置。

第十五条 公司人工智能统筹管理机构负责：制定并维护人工智能管理制度与标准；建立应用清单并组织风险分级；统筹应用准入、变更及退出管理；组织供应商评估与事件响应；受理相关咨询、投诉和申诉。

第十六条 公司各部门对本部门使用人工智能的合规性、安全性和输出质量承担直接管理责任。员工应按照公司规定，仅使用经批准的人工智能应用，并对其使用行为负责。

第四章 全生命周期与风险分级管理

第十七条 公司对人工智能应用实施统一清单管理，确保所有应用经过登记、评估和批准后方可使用，并定期核对清单。

第十八条 公司根据应用目的、决策影响、数据敏感程度、使用范围、可逆性、安全后果和受影响主体等因素，将人工智能应用分为高、中、低三个风险等级；不同风险等级对应差异化的管理要求，包括但不限于：影响评估、审批层级、技术验证、人工监督及复审安排等。公司可根据法律法规、技术发展与风险变化动态调整风险分级标准。

第十九条 公司禁止采购、部署或使用具有下列目的或后果的人工智能应用：

1. 从事法律法规禁止的活动，生成、传播违法或严重有害信息；
2. 侵害国家安全、社会公共利益或他人合法权益；
3. 以欺骗、操纵、胁迫或其他不正当方式影响他人作出重大决定；
4. 实施违法歧视、不正当竞争、价格歧视或其他不公平待遇；
5. 未经合法授权制作、传播足以使公众误认的他人声音、肖像或身份内容；
6. 绕过依法应当实施的人工审核、资格审查、安全控制或监管要求；
7. 未经授权输入、获取或披露国家秘密、商业秘密、个人信息及其他受保护数据；
8. 利用个人因年龄、残障、身心状态、教育程度、经济状况或其他脆弱处境而更易受到影响的特点，实施诱导、操纵、误导或不当施压，致使其作出可能损害自身或他人合法权益决定的；
9. 对个人实施基于社会行为、经济状况、信用表现、人格特征或其他个人特征的持续性评价、分类或排序，并据此在无关场景中给予不利待遇或者造成不成比例、不正当影响的；
10. 未经合法授权，使用人工智能开展生物特征识别、分析、追踪、监控或远程身份

识别，特别是在公共场所对个人进行实时或大规模识别监控的；

11. 其他依照适用法律法规、监管规则或公司评估认定属于禁止使用的人工智能系统。

12. 其他经评估无法将风险降低至可接受水平的情形。

第二十条 人工智能应用在采购或上线前，应当按照风险等级完成相应评估与审批。评估至少包括：

1. 应用目的、预期收益、必要性及非人工智能替代方案；

2. 受影响主体、潜在利益和不利影响；

3. 数据来源、处理范围、合法性基础、保存期限和跨境情况；

4. 准确性、可靠性、公平性、透明度和可解释性；

5. 网络安全、数据安全、权限控制和日志审计；

6. 人工监督、申诉救济、业务连续性和退出安排；

7. 供应商能力、分包安排、合同责任和知识产权风险；

8. 风险控制措施、剩余风险及责任人。

风险未降至公司可接受水平，或者不符合适用法律法规的，不得批准使用。

第二十一条 人工智能应用上线前应当在与实际用途相匹配的条件下进行测试。测试数据、方法和通过标准应与风险等级相适应，测试结果应当形成记录。高风险应用不得仅以供应商声明代替公司的独立验证。

第二十二条 人工智能输出仅可用于经批准的场景。对财务、法律、医疗健康、人力资源、安全生产、产品质量、对外披露等专业或高影响事项，使用部门应当由具备相应能力和授权的人员进行实质审核，不得直接将未经核验的输出作为最终结论。

第二十三条 应用目的、模型或供应商、部署方式、数据类别、用户范围、决策权限、接口能力或风险状况发生重大变化时，应当暂停新增使用范围并重新评估。紧急安全更新可以先行采取必要措施，但应当及时补充记录和复核。

第二十四条 公司应当持续监测人工智能应用的准确性、稳定性、偏差、投诉、安全事件和业务影响。高风险应用至少每年复审一次，并在发生重大变更、重大事件、监管要求变化或性能明显下降时及时复审。

第二十五条 出现违法违规、重大安全缺陷、持续性偏差、不可接受的错误率、供应商失去履约能力或风险无法有效控制等情形时，公司应当视情况限制、暂停或终止使用，并妥善处理数据返还、迁移、删除、账号关闭、权限回收、业务替代和记录留存。

第五章 数据、个人信息与知识产权保护

第二十六条 公司根据数据分类分级管理要求，对人工智能输入实施严格管控。员工不得向未经批准的人工智能应用输入国家秘密、商业秘密、个人信息或其他受法律保护的数据。确有业务必要处理此类信息的，应当采用经批准的受控环境，并完成相应授权、审批和保护措施。

第二十七条 人工智能应用处理个人信息时，公司应当明确处理目的、方式、范围、保存期限和合法性基础，履行告知义务并在依法需要时取得单独同意。涉及敏感个人信息、自动化决策、委托处理、对外提供或跨境提供的，应当履行适用法律规定的特别义务和影响评估要求。公司应当保障个人依法行使查阅、复制、更正、补充、删除、撤回同意、限制或拒绝处理等权利。

第二十八条 利用人工智能进行自动化决策，应当保证决策透明度和结果公平、公正。对个人权益有重大影响的决定，原则上不得仅由人工智能作出；依法可以使用自动化决策的，应当提供便捷的说明、拒绝或退出方式以及人工复核、申诉和纠错渠道。

第二十九条 公司根据风险等级采取相应的数据安全措施，包括但不限于匿名化、脱敏、加密、访问控制等。未经批准，不得利用公司数据训练、微调或改进第三方通用模型。数据保存期限届满后，应依法依约处理相关数据。

第三十条 公司应当尊重著作权、商标权、专利权、商业秘密及其他合法权益。使用人工智能生成或辅助生成内容时，应当合理核验素材来源、授权范围、许可条件和潜在侵权风险，不得将来源不明或权利状态不清的内容直接用于对外宣传、产品设计或商业交付。公司对人工智能输入、输出及相关成果的权属和使用权限，应当通过合同、制度或项目文件予以明确。

第六章 公平、透明与内容治理

第三十一条 当个人正在与人工智能系统交互，或者人工智能对其权益产生实质影响时，公司应当根据法律要求和场景风险，以显著、清晰的方式告知其人工智能的使用情况、主要目的、信息处理规则和权利途径，但法律法规规定可以不告知的除外。公司不得以披露商业秘密为由，拒绝提供法律要求的必要说明。

第三十二条 使用部门应当认识到人工智能可能生成不准确、过时、虚构或带有偏见的内容。对外发布、业务决策或专业活动中使用的人工智能输出，应当根据影响程度进行事实核验、来源核验和专业审核。

第三十三条 公司制作、发布或传播人工智能生成合成内容，应当按照适用法律法规和强制性标准添加显式、隐式或其他必要标识，不得恶意删除、篡改、伪造或隐匿依法应当保留的标识。对外发布可能使公众误认真实人物、事件或场景的生成合成内容，应当采取更加醒目的提示和审核措施。

第三十四条 公司通过适当方式公开负责任人工智能的治理原则和制度。对于依法应当公开或可能对客户、消费者、员工及其他利益相关方产生重大影响的人工智能应用，公司将根据法律要求、风险水平和商业合理性披露必要信息。公司可以结合治理成熟度和利益相关方需求发布阶段性治理进展，但不得披露国家秘密、商业秘密、个人信息或可能危及系统安全的信息。

第七章 安全、业务连续性与事件管理

第三十五条 公司将人工智能安全纳入网络安全、数据安全和全面风险管理体系，并采取适当的安全措施，防范安全风险。

第三十六条 对关键业务中的人工智能应用，公司制定与风险相适应的业务连续性、灾难恢复安排和恢复验证机制，确保应用的业务连续性。

第三十七条 公司已建立人工智能应用事件响应机制，确保在发现重大影响时，能够及时采取隔离、停用、数据保护、补救和恢复等措施。事后将进行复盘，形成整改计划并跟踪闭环。

第三十八条 公司至少每年组织一次与主要人工智能风险相适应的应急演练。关键业务部门和高风险应用供应商应当按要求参与，并根据演练结果改进响应机制。

第八章 供应商与供应链管理

第三十九条 公司在采购人工智能产品或服务前，应当根据风险等级对供应商开展尽职调查，评估其主体资质、技术能力、数据治理、网络安全、个人信息保护、知识产权、人工智能伦理、业务连续性、事件响应、分包安排和退出能力。ISO/IEC 42001、ISO/IEC 27001 等认证、第三方审计报告或安全白皮书可以作为评价证据，但不得替代公司基于具体场景开展的风险判断。

第四十条 公司应当通过合同明确供应商的服务范围、数据处理目的和方式、保密义务、安全措施、数据存储位置、跨境安排、知识产权、模型训练限制、内容标识、分包管理、审计配合、事件通知、整改、数据返还或删除、服务连续性、违约责任和退出支持。未经公司书面授权，供应商不得将公司数据用于训练、优化其通用模型或用于其他客户、产品和目的。

第四十一条 公司根据供应商风险等级开展定期评估。对处理敏感数据、支撑关键业务或影响重大权益的供应商，可以通过问卷、材料核验、技术测试、访谈或现场审计等方式实施监督。供应商出现重大违规、安全事件、拒绝合理审计、持续不符合整改要求或履约能力严重下降时，公司可以依法依约要求整改、限制新增业务、暂停服务或终止合作，并依法向有关部门报告。

第九章 人工智能管理策略

第四十二条 公司建立分层分类的人工智能培训机制，覆盖新员工、全体员工及高风险应用相关人员。培训内容包括适用规则、数据安全、公平性、知识产权、人工核验及事件报告等。公司通过测试、演练等方式验证培训效果。

第四十三条 公司至少每年开展一次人工智能治理内部检查或审计，并根据风险、监管要求和事件情况安排专项审计或独立评估。检查或审计发现的问题应当明确责任人、整改措施和完成期限，并持续跟踪至闭环。公司依法配合监管部门的监督检查，并要求相关供应商提供必要协助。

第四十四条 违反本制度的，公司根据行为性质、主观过错、影响范围、损害后果和整改情况，依照公司规章制度采取提醒、培训、责令整改、权限限制、纪律处分或追究损失等措施；涉嫌违法犯罪的，依法移交有关机关处理。

责任追究应当以事实为依据、程序正当、尺度适当。主动报告风险、及时采取补救措施并有效减轻损害的，可以依法依规酌情处理。

第四十五条 公司通过官方网站、客户服务渠道或另行公布的合规渠道，受理与人工智能应用有关的咨询、投诉、举报和申诉，并公布或提供相应的处理流程和反馈方式。公司应当及时、公正处理相关事项，保护投诉人、举报人和申诉人的个人信息及其他合法权益。任何单位或个人不得对善意提出问题、报告风险或参与调查的人员实施打击报复。

第十章 附则

本制度由可持续发展领导组审议通过，自可持续发展领导组审议通过之日起生效。本规则的修改事项应经可持续发展领导组审议通过。

本制度解释权归公司可持续发展领导组。

稳健医疗用品股份有限公司

2026 年 8 月 3 日