碳离子/质子治疗系统

软件系统检查要点

国家药品监督管理局食品药品审核查验中心

2025 年 12 月

目　录

碳离子/质子治疗系统

软件系统检查要点

一、产品介绍

碳离子/质子治疗系统中软件系统主要包括加速器控制系统、肿瘤信息系统、治疗计划系统和治疗控制系统四个部分，以实现加速器控制、肿瘤信息管理、治疗计划管理和治疗端控制。

（一）加速器控制系统

1. 功能介绍。本系统作为加速器控制系统的核心可视化平台，集操作、监控、分析与诊断功能于一体。通过与控制设备协同工作，实现了对磁铁电源、真空系统等子系统的实时监控，同时提供定时触发、联锁保护与中央监控等核心功能，并为操作人员提供直观的可视化人机交互界面。软件实时显示加速器各设备的运行参数、状态信息及故障报警等，支持对设备参数、运行状态及历史数据的存储、检索与分析，为调试和运维团队提供在线监测与分析工具。

2. 结构组成。通常包括中央定时系统、电源系统监控、联锁系统、真空系统监控、冷却水监测、系统管理等模块，各模块之间基于中央监控系统的集成进行数据交互，实现对加速器系统相关设备的集成调试与监测。

（二）肿瘤信息系统

1. 功能介绍。本系统作为集成化肿瘤治疗管理平台，主要用

于管理患者治疗全流程、处理治疗计划、校验机器参数、记录与验证治疗数据，并对患者影像及剂量评估结果进行统一管理与审核，最终将各类医疗信息汇总生成完整的肿瘤学专用电子病历，实现便捷查询与集中管理，以全面支持医疗信息管理工作。同时通过多权限用户间的协同交互与流程控制，完成从治疗规划到执行的全过程管理，并与医院 PACS 系统集成，实现对患者影像的调取、存储与展示。

2. 结构组成。通常包括临床病历、影像管理、DICOM 传输、数据存储、治疗验证和记录、治疗计划和影像审核、患者排程叫号、流程表单、数据统计等模块。

（三）治疗计划系统

1. 功能介绍。本系统作为专业的放射治疗计划设计与分析平台，主要用于模拟放射治疗对患者的辐射作用。通过软件建立放射治疗设备的物理与几何模型，导入患者医学影像后，结合机器模型参数与内置剂量计算算法，完成治疗计划的设计与剂量分布计算，经评估确认合格的计划与剂量分布将被传送至放射治疗设备，用于实施患者治疗。此外，系统还可基于治疗过程中产生的医学影像，计算并跟踪剂量偏差，及时修正治疗计划，确保治疗的精准性与安全性。

2. 结构组成。通常包括患者数据管理、患者建模、计划设计、计划优化、计划评估、QA 准备、自动计划、脚本设计、生物模型管理、物理数据管理、系统管理、报告设计等模块。

（四）治疗控制系统

1. 功能介绍。本系统是放射治疗执行阶段的核心平台，负责引导临床用户完成标准治疗工作流程，并协同各子系统运作，包括获取与显示患者信息及治疗计划，实时监控各治疗室与治疗设备的运行状态，控制治疗头、治疗床等关键设备以执行患者摆位、束流申请与患者照射。在此过程中实时显示治疗数据与设备联锁状态，并最终记录与归档治疗过程数据。

2. 结构组成。通常包含以下六大模块：信息管理模块，如用户登录、摆位计划推送、照射计划推送、摆位验证、实时照射数据、照射报告提交；图像引导定位和呼吸运动管理模块，如启动定位、定位结果、定位完成、启动呼吸运动跟踪；照射控制模块，如照射计划推送、实时照射数据、运行指令；治疗床调整模块，如摆位调整、运动状态、摆位结果；机架调整模块，如机架调整、运动状态、机架结果；治疗流程模块，如计划获取、摆位调整、束流申请、启动照射、照射报告。

（五）四个软件的相互关系

四个软件构成了一个紧密协作的治疗闭环。其中，肿瘤信息系统作为信息中枢与流程管理，全面管理患者治疗流程，并作为中央数据库连接诊断与执行。治疗计划系统是承上启下的方案设计者，其将医学目标转化为可执行的物理指令，并将设计好的治疗计划传输至治疗控制系统。治疗控制系统是核心治疗执行与调度接口，其解析治疗计划并生成设备指令，同时监督治疗全过程，

确保计划被准确无误地执行。最终，由加速器控制系统接收治疗控制系统指令，控制加速器产生离子束流用于肿瘤患者治疗。治疗结束后，治疗过程数据存入肿瘤信息系统。整个网络通过紧密的数据交换，不仅实现了从临床决策到设备执行的信息流闭环，而且构建了从设备状态回溯到控制系统的安全监督闭环，共同确保了放射治疗的安全、精准与高效。

二、主要技术指标

序号	检验项目		主要控制指标
1	软件环境		软件系统运行环境的说明，包括服务端、客户端的软件环境和硬件环境及网络环境
2	功能	加速器控制系统	电源监控、真空监控、中央定时、中央联锁、用户管理、数据存储等
3		肿瘤信息系统	排程、治疗报告、点扫描/均匀扫描标定审核、计划管理、摆位报告、TPS 剂量修正、用户管理、记录与验证等
4		治疗计划系统	患者管理、患者建模、计划设计、计划优化、计划评估、QA 和配置管理等
5		治疗控制系统	显示功能（显示治疗计划中的患者信息、治疗床和机架的位置信息、辐射剂量信息、剂量率信息、治疗状态和系统联锁状态）、患者治疗功能（启动照射、中断辐照、终止辐照、继续辐照、上传照射数据）
6	性能		软件系统易用性、可靠性、兼容性、性能效率、可维护性、可移植性、信息安全性等
7	使用限制		软件的用户使用限制
8	数据管理		数据传输、数据接收、删除和编辑数据、数据备份、数据归档等
9	用户访问控制		登录用户名和密码，以及用户权限区分的说明

三、生产和质量关键控制点

（一）生产风险环节

软件系统生产风险环节包括需求管理、开发环境、软件设计、软件验证、数据安全、配置管理及安装部署等。

（二）质量管理关键控制措施

序号	风险环节	主要风险点	控制措施
1	需求管理	①用户需求、产品需求等不明确或不充分，导致软件设计不满足要求; ②新增的个性化需求沟通不充分，导致最终产品与用户预期不符。	①企业应当依据软件设计开发程序文件的要求进行软件策划、需求分析。用户需求、产品需求、法规/标准要求、风险管理要求等输入信息应当充分; ②对于新增的个性化需求，企业应当主动和用户保持沟通，记录沟通结果，并将每一阶段的产品及时与其确认。
2	开发环境	①开发测试环境维护不当，如未定期验证、更新、病毒查杀等，导致开发基础不可靠; ②开发工具、测试工具或检测设备中的计算机软件未经确认或确认不当，影响开发过程与结果的有效性; ③开发团队使用的工具及版本不统一、不规范，导致协作混乱或构建结果不一致。	①企业应当配备软件开发测试环境，建立软件开发测试环境维护文件及相应的维护记录，如定期验证、更新升级、病毒查杀记录等; ②企业应当制定计算机软件确认程序文件，依据文件要求对软件开发工具（如配置管理工具和自研或第三方软件测试工具等）、安装在检测设备中的计算机软件进行确认，当软件更改、受计算机病毒侵害等情况发生时，企业应当进行再确认; ③软件研发负责人或软件架构师应当对开发团队使用的工具及版本等进行统一规范、管理，

序号	风险环节	主要风险点	控制措施
			并进行确认。
3	软件设计	①缺乏软件设计开发规范指导，导致设计过程无序，软件存在质量风险; ②软件设计未能满足输入的国家和行业标准等要求; ③软件设计变更控制不当，可能导致未经充分验证的变更影响医疗器械的安全性或有效性; ④软件设计缺乏可追溯性，导致问题难以定位、影响范围难以评估; ⑤使用未知来源现成软件可能引入未知的安全风险。	①企业应当建立软件设计开发规范; ②软件设计应当满足输入的国家和行业标准等要求; ③软件设计变更应当进行识别、验证和评审等，对于重大增强类软件更新，影响到医疗器械安全性或有效性的增强类更新，发布版本变更的，应进行注册变更; ④软件设计应当建立可追溯性机制，形成可追溯性记录，如从测试追溯到源代码，从源代码追溯到设计，从设计追溯到需求; ⑤企业应当对现成软件（尤其是未知来源软件）的风险进行评估，并采取安全措施确保软件安全。
4	软件验证	①缺乏系统性的测试计划或计划未经评审，导致测试覆盖不全或重点偏离; ②测试用例设计不完善或未经评审，无法有效验证软件功能与性能; ③测试工具本身不稳定或不可靠，影响测试结果的准确性和可信度; ④未按测试用例严格执行各项测试，或测试记录/报告不真实、不完整，无法证明软件符合要求; ⑤软件标识不清晰或不完	①企业应当建立软件测试计划，包括单元测试、集成测试、系统测试、网络安全测试，并对其进行评审; ②企业应当制定软件测试用例，并对其进行评审，检查测试用例覆盖情况; ③企业应当选择成熟稳定可靠的测试工具; ④企业应当依据软件测试用例对软件进行单元测试、集成测试、系统测试、网络安全测试，测试报告、自检报告应当满足真实、完整性要求;

序号	风险环节	主要风险点	控制措施
		整，导致版本混淆，难以实现追溯。	⑤软件标识应当满足可追溯性要求，如软件名称、规格型号、完整版本、发布版本、HASH值等。
5	数据安全	①软件系统电子接口访问控制不当，存在非授权访问或使用的风险; ②软件面临网络安全威胁（如网络攻击、未授权访问），缺乏有效的防护、检测与响应机制; ③软件系统存在未知漏洞，可能被利用从而危及系统安全与患者安全; ④患者敏感信息在系统中明文显示或处理不当，存在泄露风险，违反隐私保护要求; ⑤重要数据缺乏有效的备份与恢复机制，在灾难或故障发生时可能导致数据永久丢失。	①企业应当对软件系统电子接口（如网络接口、电子数据交换接口）的访问、防护等进行控制，防止非预期的使用; ②企业应当对软件网络安全威胁进行识别、保护、探测、响应、恢复等，如采用防火墙、堡垒机、漏洞扫描系统、终端用户管理系统等硬件防护措施，网络安全具体参照《医疗器械网络安全注册审查指导原则》; ③企业应当对软件系统漏洞进行扫描，如根据软件安全性级别进行网络安全漏洞自评或第三方漏洞评估检测，且两者不能使用同一工具进行漏洞扫描; ④企业应当对软件系统患者数据进行去标识化与匿名化处理，患者姓名、年龄、身份证号、手机号、照片等敏感信息应当被匿名化处理; ⑤企业应当对软件系统重要数据进行备份，备份方案设计合理，如异地增量备份，便于数据的备份与恢复等。
6	配置管理	①缺乏软件配置管理程序文件，导致配置管理活动无据可依;	①企业应当建立软件配置管理程序文件; ②企业应当依据配置管理程序

序号	风险环节	主要风险点	控制措施
		②软件版本、源代码、文件、工具、现成软件等配置项未受控，状态混乱; ③配置项未得到有效识别、标识和检查，可能导致使用错误的版本或组件; ④配置状态不清晰，无法准确了解软件开发过程中的基线状态和版本迭代; ⑤软件版本变更失控，变更未经过充分的验证和评审，可能引入新的风险。	文件要求对软件版本、源代码、文件、工具、现成软件等进行控制; ③企业应当对软件配置项进行识别、标识，QA 对配置项进行检查，记录检查结果; ④QA 根据软件开发阶段检查配置状态，并对配置状态进行记录及更新; ⑤企业应当对软件版本变更（涵盖软件、网络安全的全部更新）进行控制，并保留变更记录、验证记录。
7	安装部署	①现场运行环境与软件技术要求不符，导致软件无法正常运行或性能不稳定; ②发行的软件版本与源代码版本无法对应，导致问题追溯和版本维护困难; ③现场安装的软件版本来源不受控，可能安装了未经授权的或错误的版本; ④软件安装后未进行充分确认及测试，无法保证安装的正确性。	①现场安装人员应当根据当前软件系统的技术要求，核对现场的运行环境是否与技术要求一致; ②版本管理人员或配置管理人员应当对发行的每个软件版本进行跟踪检查，确保能追踪到当前版本所对应的源码备份; ③现场安装的软件版本出口应当统一，统一由版本管理人员或配置管理人员从受控库检出再转交给软件安装人员; ④现场软件安装完成后应当进行确认及测试，形成安装记录。

四、检查要点

（一）机构与人员

企业应当建立与软件系统相适应的组织机构、配备相适应的人员，明确关键岗位人员职责，以保证软件的研发、生产和质量

控制满足要求。

1. 关键岗位人员

（1）开发人员。应当配备具有软件工程基础、数据库专业知识、系统架构与集成、网络和安全技术等专业知识的技术和设计人员。

（2）测试人员。应当配备单元测试、集成测试、系统测试等专职测试人员，应当熟悉医疗器械相关法律法规、标准、技术要求、检验方法及仪器操作方法。同一软件项的开发人员和测试人员不得互相兼任。

2. 人员能力

应当对从事影响软件质量的关键岗位人员制定考核评价制度，培训内容应当包括医疗器械相关法律法规、软件需求规范、测试用例等，并保留相关培训记录。

软件开发和测试人员应当具备与岗位职责要求相适宜的专业知识、实践经验和工作能力。

（二）厂房与设施

企业应当配备与软件系统相适应的机房，具备适当的照明、温度、湿度和通风控制条件，以及防水、防静电等防护措施。

机房应当有足够的空间，并与硬件规模相适应。机房的管理应形成文件，对访问人员、网络安全、消防安全等要求进行规定并保持相关记录。涉及第三方机房的，应当按照采购要求进行管理。

（三）设备

企业应当在软件生存周期过程中持续提供充分、适宜、有效的软件开发和测试环境，包括软硬件设备、开发测试工具、网络等资源以及病毒防护、数据备份与恢复等保证措施。

设备包括硬件与网络，如服务器、网络存储、交换机/防火墙；软件平台，如版本控制系统、集成/部署工具；开发与构建工具，如编程语言/编译器、构建工具、数据库管理系统；管理与协作工具，如缺陷管理工具、配置管理工具；测试软件与工具，如测试管理工具、自动化测试工具、安全测试工具等。

（四）文件和数据管理

企业应当根据软件系统生产实际情况，建立健全相应的研发、生产和质量控制管理文件。

1. 应当建立与软件生产相适应的技术和管理文件，并保持相关记录。技术文件应当包括软件技术指标及相关标准、软件需求、软件设计、软件测试等文件。记录应当确保软件开发过程可追溯。

2. 采用数字化、信息化管理方式的，应当确保电子记录或者数据真实、准确、及时、完整和可追溯。

（五）设计开发

企业应当结合软件生存周期模型特点建立软件生存周期过程控制程序并形成文件，确定软件开发策划、软件需求分析、软件设计、软件编码、验证与确认、软件更新、风险管理、缺陷管理、可追溯性分析、配置管理、文件与记录控制、现成软件使用、

网络安全保证、软件发布、软件部署、软件停运等活动要求。

1. 软件开发策划

软件开发策划应当确保与软件开发要求相适宜的开发和测试人员及环境，并确定软件需求分析、软件设计、软件编码、软件测试、风险管理等活动的计划，形成相关文件和记录。风险管理活动应当结合软件功能、接口、用户界面、现成软件、网络安全等进行风险识别、分析、评价、控制和验证，并贯穿于软件生存周期全过程。

2. 软件开发

（1）应当对软件需求进行分析，包括法规、标准、用户、产品、功能、性能、接口、用户界面、网络安全、警示提示等内容，确定风险管理、可追溯性分析、现成软件使用评估、软件确认测试计划创建、评审等活动要求，形成软件需求规范和评审记录并经批准。软件需求规范应当包含软件内各功能的数据流图、体现软件组件的组织结构和依赖关系的组件图、用户界面关系图等。

（2）应当依据软件需求规范实施软件体系架构、功能、性能、算法、接口、用户界面、单元、网络安全等设计，形成软件设计规范和评审记录并经批准。软件设计规范应当包含软件系统架构图，如体现软件系统整体结构和组件关系的顶层架构图、描述系统的逻辑分层和职责划分的逻辑架构图、物理架构图等。

（3）应当依据软件设计规范进行软件编码，确定源代码编

写与注释、现成软件使用、可追溯性分析、各级测试用例创建、评审等活动要求，形成评审记录。源代码编写与注释应当符合软件编码规则文件的要求。

（4）应当建立软件配置管理控制程序并形成文件，规范软件版本、源代码、文件、工具、现成软件等控制要求，确定配置标识、变更控制、配置状态记录等活动要求。使用配置管理工具保证软件质量，并贯穿于软件生存周期全过程。

（5）应当根据软件产品特点、质量管理体系要求、合规性等因素制定软件版本命名规则并予以记录，各字段含义明确且无歧义无矛盾。

3. 验证与确认

（1）应当制定软件测试计划，依据软件测试计划进行单元测试、集成测试、系统测试，涵盖现成软件、网络安全的测试要求，形成相应软件测试记录、测试报告以及评审记录，并适时更新，且应当对测试数据进行复核。

（2）应当制定软件确认制度，确认内容包含用户测试、临床评价、评审等活动要求，涵盖现成软件、网络安全的确认要求，并保持相关记录，能够保证软件满足用户需求和预期目的。

（3）应当对软件系统中涉及患者安全与治疗精度的核心算法如治疗计划相关接口与数据处理算法、治疗流程管理与优化算法、数据管理与分析算法等进行专项验证，确保其准确性、可靠性与一致性。验证活动需涵盖算法原理正确性、典型用例与边界

数据测试、临床一致性比对、性能效率及变更影响评估。

4. 可追溯性分析

应当建立软件可追溯性分析控制程序并形成文件，涵盖现成软件、网络安全的控制要求，软件可追溯性分析能够追踪到软件需求、软件设计、源代码、测试及风险管理之间的关系，相互之间满足正确性、一致性和完整性的要求。

5. 缺陷管理

应当建立软件缺陷管理制度，对软件开发及使用过程中发现的各类缺陷（如非预期输入数据的响应、数据库、操作系统、IT环境等外部组件的错误、网络安全风险/威胁、人机界面和人为错误等）进行记录、评估、修复、回归测试、风险管理、评审等，形成软件缺陷分析报告，并确保已知剩余缺陷的风险均可接受。

6. 变更控制

（1）软件更新应当形成文件，涵盖现成软件、网络安全的变更控制要求，确定软件更新请求评估、软件更新策划、软件更新实施、风险管理、验证与确认、缺陷管理、可追溯性分析、配置管理、文件与记录控制、评审、用户告知等活动要求。

（2）软件版本变更应当与软件版本命名规则相匹配，并根据软件更新的类型、内容和程度实施相适宜的回归测试、用户测试等活动，必要时应当申请变更注册。如软件发生新增临床功能（如动态靶区跟踪）、新增核心算法模块（如AI器官自动分割）、架构重构（如单机版升级为云原生）、关键接口不兼容变更（如

与 HIS/PACS 的交互协议）、安全架构重大调整（如引入双因素认证）等重大增强类更新，应当申请变更注册。

7. 网络安全

（1）应当确保网络安全需求、网络安全设计、源代码、网络安全测试、网络安全风险管理等文档可追溯，且文档间相关信息一致、完整、准确。

（2）应当结合软件网络安全特性开展网络安全验证与确认活动并保留验证相关文件，可选择源代码安全审核、威胁建模、病毒扫描、漏洞扫描、渗透测试、模糊测试等进行验证，其中漏洞扫描是必须开展的软件验证活动。

（六）采购

企业应当建立采购控制程序，确保采购的原材料或者服务，包括现成软件（遗留软件、成品软件、外包软件）、云计算服务等，以及采购原材料及服务的更新等符合相关要求，且不低于法律法规和强制性标准的要求，并能实现追溯。

1. 应当建立供应商评价与选择准则，覆盖现成软件供应商、云计算服务商等，供应商应当具备相应的资质、软件开发能力和质量保证能力等。应当与供应商签订质量协议，明确双方承担的质量责任，并根据采购原材料或服务对产品的影响程度，对供应商进行分类管理和控制。

2. 应当明确现成软件的采购要求，包括关键技术指标、交付形式、验收方式与准则、更新维护等内容，并保留采购记录，包

括采购合同或软件开发合同、软件开发文档等，采购记录应当真实、准确、完整和可追溯。

3. 应当对采购现成软件的关键技术指标进行检验或验证，包括版本号、软件功能、兼容性等，并按照软件验证与确认的要求进行必要的测试，确保软件满足采购要求。

4. 应当与供应商建立良好的沟通机制，明确软件变更时的沟通流程、责任与响应时限，确保软件功能、算法、接口等关键内容发生变更时，供应商能够及时提供变更信息的完整说明，包括详细的变更内容、风险评估及验证确认措施，同时企业应当及时确认变更内容，评估变更的影响，必要时进行验证与确认，并保留沟通记录和变更记录。

（七）生产管理

企业应当建立生产过程控制要求，明确软件发布和软件交付要求，并按照要求组织生产。

1. 软件发布应当形成文件，确定软件文件创建、软件与文件归档备份、软件版本识别与标记、交付形式评估与验证、病毒防护等活动要求，保证软件发布的可重复性。

2. 软件交付形式主要包括网络交付与物理交付两种方式。物理交付方式应当确定软件产品复制、许可授权以及存储媒介包装、标记、防护等要求；网络交付方式应当确定软件产品标记、许可授权、网络安全保证等要求。

（八）质量控制

企业应当建立质量控制程序，明确软件质量控制要求，确保产品在放行前完成规定的检验，满足质量控制要求。

1. 软件功能检验项目应当包括:

（1）加速器控制系统：电源监测、真空监测、中央定时、联锁监控、用户管理、数据存储等。

（2）肿瘤信息系统：排程功能、治疗报告功能、调制扫描/均匀扫描标定审核功能、计划管理功能、摆位报告功能、TPS 剂量修正功能、用户管理、记录与验证报告等。

（3）治疗计划系统：患者管理、患者模型、计划设计、计划优化、计划评估、QA 和配置管理等。

（4）治疗控制系统：显示功能及患者治疗功能，显示功能包括显示治疗计划中的患者信息、治疗床和机架的位置信息，显示辐射剂量信息、剂量率信息、治疗状态和系统联锁状态；患者治疗功能包括启动照射、中断辐照、终止辐照、继续辐照等。

2. 软件放行应当形成文件，确定软件版本识别、产品完整性检查、放行批准等活动要求，并保持相关记录。

（九）软件部署和维护

企业应当建立软件部署和维护的控制程序，确保软件质量安全和运行稳定。

1. 软件部署应当形成文件，确定交付、安装、设置、配置、用户培训等活动要求，保持相关记录。软件安装应当确认硬件配置、运行环境、网络条件等，确保满足安装要求。

2. 应当在软件维护控制程序中明确使用过程中持续性验证与维护的要求:

（1）加速器控制系统

维护活动应当与加速器的物理部件维护计划同步。在硬件组件更换或重大维修后，应当对控制软件进行功能性再确认，重点关注时序错误和硬件故障代码。

（2）肿瘤信息系统

验证其与 HIS、PACS 等外部系统间数据接口的兼容性与数据完整性。任何关联系统升级后，都应当进行回归测试，确保患者信息、治疗计划、影像数据等在不同系统间传输无误。

维护工作包括数据管理与性能优化。应当定期进行数据库维护，并监控系统在大量病例数据时的响应速度。用户权限审计是维护的关键环节，以防越权访问。

（3）治疗计划系统

任何更新或环境变化后，应当进行剂量计算准确性验证，将计算结果与已知标准模型或测量数据进行比对，确保剂量计算的准确性。对于自动计划、生物模型等功能，应当建立针对性的验证流程。

维护工作包括物理数据管理和算法模型维护。当引入新的治疗技术时，应当评估现有软件模型是否支持，必要时进行升级和全面验证。

（4）治疗控制系统

验证应当覆盖完整的治疗工作流程。紧急中断功能的测试应当在每次重大更新后进行。

维护应当关注其与所有子系统（如加速器控制系统、肿瘤信息系统、影像设备等）的通信链路状态，确保治疗记录数据的完整与不可篡改。

3. 应当建立网络安全事件应急响应团队，制定网络安全事件应急响应预案，在运行维护过程中通过漏洞评估识别相关网络安全事件，在事件发生期间及时告知用户应对措施。

4. 软件停运应当形成文件，确定停运后续用户服务、数据迁移、患者数据与隐私保护、用户告知等活动要求，并保持相关记录。