附录3:

控制系统检查要点

1. 肿瘤信息系统

（征求意见稿）

一、产品介绍

（一）预期用途

适用于用户在碳离子/质子治疗系统中管理患者治疗流程、治疗计划、机器参数校验、验证和记录治疗数据、管理和审核影像以及进行剂量评估。

（二）工作原理

肿瘤信息系统将信息汇总成一个完整的肿瘤学专用电子病历，便于查询和管理，以支持医疗信息管理；通过不同权限、不同用户之间的交互和流程管理，完成整个患者治疗的全流程管理；与医院影像归档和通信系统（PACS）交互，管理、存储和展示患者影像。

（三）结构组成

本产品通常由临床病历、影像管理、DICOM、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、数据统计等模块组成。

1. 主要技术指标

| **序号** | **检验项目** | **主要控制指标** | **检验方法** |
| --- | --- | --- | --- |
|  | 软件环境 | 技术文件中应提供肿瘤信息系统运行环境，包括：服务端、客户端的软件环境和硬件环境及网络环境 | 按照企业制定的规程 |
|  | 临床功能 | 技术文件中应提供肿瘤信息系统临床功能，包括：肿瘤信息系统功能（排程功能、治疗报告功能、点扫描/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、记录与验证等 | 按照企业制定的规程 |
|  | 使用限制 | 技术文件中应提供肿瘤信息系统用户使用限制 | 按照企业制定的规程 |
|  | 数据接口 | 技术文件中应提供肿瘤信息系统数据交互接口 | 按照企业制定的规程 |
|  | 用户访问控制 | 技术文件中应提供肿瘤信息系统软件登录用户名和密码，以及用户权限区分 | 按照企业制定的规程 |
|  | 性能 | 技术文件中应提供肿瘤信息系统软件易用性、可靠性、兼容性、性能效率、维护性、可移植性、信息安全性等 | 按照企业制定的规程 |

三、生产工艺和质量关键控制点

（一）生产环节风险点

肿瘤信息系统生产环节风险点主要包括人员、需求、开发环境、软件设计、软件验证、数据安全、配置管理、安装等。

（二）生产质量管理关键控制措施

| **序号** | **风险点** | **控制措施** |
| --- | --- | --- |
| 1 | 人员 | ①企业应配备软件架构师、算法工程师、软件开发工程师、软件测试工程师、UI工程师等技术人员；②软件开发、测试、维护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，应保证黑盒测试同一软件项的开发人员和测试人员不得互相兼任；③企业应在设计开发周期内关注团队人员的状态，建立人才储备；④企业应对软件开发人员和测试人员进行需求规范、设计规范、使用说明书、标准等的培训。 |
| 2 | 需求 | ①选择熟悉肿瘤信息系统业务的人员担任核心的设计开发；②对新员工制定培训计划，进行业务培训，培训合格即可参与系统的设计开发测试工作；③对于项目中新增的个性化需求，应主动和最终用户代表保持沟通，记录沟通结果；并将每一阶段的成果物及时和其确认。 |
| 3 | 开发环境 | ①企业应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（定期验证、更新升级、病毒查杀记录等）；➁企业应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，企业应进行再确认；③软件研发负责人或软件架构师应对开发团队使用的工具及版本等进行统一规范、管理，并进行确认。 |
| 4 | 软件设计 | ①企业应建立软件设计开发程序文件；➁企业应依据软件设计开发程序文件的要求进行软件策划、需求分析及设计；③软件设计开发输入的用户需求、自身需求、预期用途的功能、性能、安全要求、法规/标准要求、风险管理要求等输入信息应充分；④软件设计开发输出的技术要求应满足输入的国家和行业标准等要求；➄软件设计变更应进行识别、提出、验证和评审等，发布版本变更的，应进行注册变更；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；➅软件开发过程应建立可追溯性机制，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；⑦企业应对现成软件（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。 |
| 5 | 软件验证 | ①企业应建立软件测试计划（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；➁企业应制定软件测试用例，并对其进行评审，检查测试用例覆盖情况；③企业应选择成熟稳定可靠的测试工具；④企业应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，测试记录、测试报告、自检记录、自检报告应满足真实、完整性要求；➄软件标识应满足可追溯性要求，如软件名称、规格型号、完整版本、发布版本、HASH值等。 |
| 6 | 数据安全 | ①企业应对软件系统电子接口（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；➁企业应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企业应对软件系统患者数据进行去标识化与匿名化处理，敏感信息如患者姓名、年龄、身份证号、手机号、照片等不直接在系统中明码完整显示；➄企业应对软件系统重要数据进行灾备，灾备方案设计合理，如异地增量备份，便于数据的备份与恢复等。 |
| 7 | 配置管理 | 企业应建立软件配置管理程序文件；➁企业应依据配置管理程序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；➄企业应对软件版本变更（涵盖软件、现成软件、网络安全的全部更新）进行控制，并保留变更记录、验证记录。 |
| 8 | 安装 | 1. 现场安装人员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；

➁由版本管理人员或配置管理人员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必须统一，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须进行确认及测试，形成安装记录。 |

四、检查要点

（一）机构与人员

查看企业是否对从事影响产品质量的工作人员，特别是产品设计开发人员、测试人员等制定考核评价制度，培训内容是否包含相关法律法规、基础理论知识、专业操作技能、过程质量控制及质量检验等，并保留相关培训记录。如：软件设计开发人员和测试人员需进行强制性标准及行业标准IEC 62304（YY/T 0664）等培训。

（二）厂房与设施

企业应从多个方面进行考虑，包括硬件设施、软件设施、环境要求等。

1．企业应配备相应的硬件设备，包括处理器、内存、存储设备、服务器及测试设备等；

2．企业应配备相应的软件设施，包括操作系统（如Windows等）、开发工具（如集成开发环境等）、测试工具（如Selenium、Junit等）、项目管理工具、版本控制系统等；

3．企业应确保其生产环境满足要求，厂房通风良好、光照充足，并保持适宜的温度与湿度。机房内空气含尘浓度需低于规定标准，同时必须配备有效的接地系统和高可靠性的供电系统。

（三）设备

企业应在肿瘤信息系统软件开发过程提供充分、适宜、有效的开发和测试环境，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。

软件开发和测试环境维护应形成文件，确定软件开发和测试环境定期验证、更新升级、病毒防护等活动要求，保持相关记录。

（四）文件管理

此部分内容详见总则要求。

（五）设计开发

1.企业应依据风险管理控制程序实施软件风险管理活动，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。

（1）企业应在肿瘤信息系统软件设计开发策划阶段制定软件风险管理计划，包括风险管理活动的范围、职责和权限的分配、风险管理方针、风险可接受性准则、风险管理活动计划、验证活动、生产和生产后信息的收集等。

（2）企业应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，例如：非预期输入数据的响应，使用的外部组件的错误（比如数据库、操作系统和IT环境），网络安全风险/威胁、人机界面和人为错误等。

2.企业应根据软件产品特点、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。例如，软件版本命名规则为X.Y.Z.B，其中X表示重大增强类更新，Y表示轻微增强类更新，Z表示纠正类更新，B表示内部构建，则软件完整版本为X.Y.Z.B，而软件发布版本为X，此时X发生变化应进行许可事项变更，而Y、Z和B发生变化无需进行许可事项变更。

3.企业应建立软件可追溯性分析控制程序并形成文件，应涵盖现成软件、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。

4.企业应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、警示提示等软件需求，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，应形成软件需求规范和评审记录并经批准，适时更新并经批准。

5.企业应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，确定风险管理、可追溯性分析、现成软件使用评估、软件验证测试计划创建、评审等活动要求，形成软件设计规范和评审记录并经批准，适时更新并经批准。

6.企业应制定软件测试计划，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。

7.企业应制定软件确认制度，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，且软件已知剩余缺陷的风险均可接受。

8.企业软件更新应形成文件，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，形成相关文件和记录并经批准，适时更新并经批准。软件版本变更应当与软件更新情况相匹配。验证与确认应当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。

（六）采购

此部分内容详见总则要求

（七）质量控制

1. 企业应建立软件检验管理制度，依据检验制度对软件进行相应测试，并保留相关记录。
2. 企业应建立软件产品放行文件，确定软件版本识别、安装卸载测试、产品完整性检查、放行批准等活动要求，并保留相关记录。
3. 不合格品控制
4. 企业应建立不合格品控制程序，规定不合格品控制的部门和人员的职责与权限。
5. 企业应明确不合格物料的识别、记录、隔离和评审流程，根据评审结果，对不合格物料采取相应的处置措施。
6. 企业应按程序文件要求执行，对不合格物料分门归类、原因分析、纠正预防措施应合理、有效，应进行评审，且保留评审记录。
7. 企业应对可以返工的不合格物料作出规定，应按照返工文件要求进行返工活动，并记录。
8. 企业应建立不合格物料处置记录，记录内容应完整且能有效反映处置的过程，满足可追溯要求。