

医疗器械独立软件现场核查指南

一、目的

本指南是对上海市医疗器械独立软件（以下简称独立软件）产品开展现场检查的指导性要求。旨在帮助医疗器械检查员梳理、把握独立软件的软件生存周期特征及核查要求，统一检查尺度。同时，也为本市独立软件注册申请人建立及运行质量管理体系的工作提供参考。本指南目的在于进一步提升本市独立软件生产监督检查效能，不作为法规强制执行。注册申请人应依据申报产品的实际情况，遵循相关法规要求建立质量管理体系并保持有效运行。

二、适用范围

本指南适用于第二、三类独立软件现场体系核查，包括企业自行开发的软件。

三、医疗器械独立软件概要

（一）医疗器械独立软件

医疗器械独立软件（简称独立软件）是指本身即为医疗器械的软件。它有一个或多个医学诊疗目的，运行于通用计算平台上，无需医疗器械硬件的支持即可完成预期用途。通用计算平台须满足信息技术设备安全要求（含电磁兼容）。独

立软件可分为通用型和专用型两大类，前者通常基于通用数据接口与多个医疗器械联合使用；后者基于通用、专用数据接口与特定医疗器械联合使用，可视为医疗器械附件。

独立软件不具有物理实体，在开发、使用以及维护过程中人为因素的影响无处不在。由于时间和成本的限制，软件测试无法穷尽所有可能的情况，因此软件缺陷无法避免，软件的轻微更新也可能会导致严重后果。另外，软件的累积效应和退化问题（即每修复若干个缺陷就会产生一个新缺陷）也会导致软件缺陷无法根除。因此，软件缺陷可视为软件的固有属性之一，软件的质量问题不容忽视。鉴于上述软件特性，应综合考虑软件工程、质量管理及风险管理的要求，以保证软件的安全有效。

（二）运行支持软件

独立软件属于应用软件，其正常运行通常需要基于系统软件，或同时需要应用软件（含其他医疗器械软件）、中间件、支持软件的支持。运行所需主要支持软件详见表 1。

表 1 运行所需主要支持软件

名称	定义	举例
系统软件	用于保障计算机系统正常运行的软件	操作系统软件、虚拟机软件
应用软件	用于实现计算机用户特定需求的软件	浏览器软件、数据库软件、安全

		软件
中间件	介于系统软件和应用软件之间，依赖于系统软件的支持，同时又为应用软件提供支持的软件	分布式计算平台软件
支持软件	用于开发、测试其他软件的软件	软件开发工具、软件测试工具

四、医疗器械独立软件产品实现过程

（一）软件生存周期

软件生存周期（又称软件生命周期）是指软件系统从概念定义至停止使用的时间周期，包括软件开发策划、软件开发过程、软件部署、软件维护、软件停运等阶段。

软件产品通过开发过程实现，软件开发过程为软件生存周期过程中最为关键、核心的过程。软件开发过程主要包括软件需求分析、软件设计、软件编码、软件验证、软件确认、软件发布等系列活动。该过程由图 1 所示的若干活动组成。

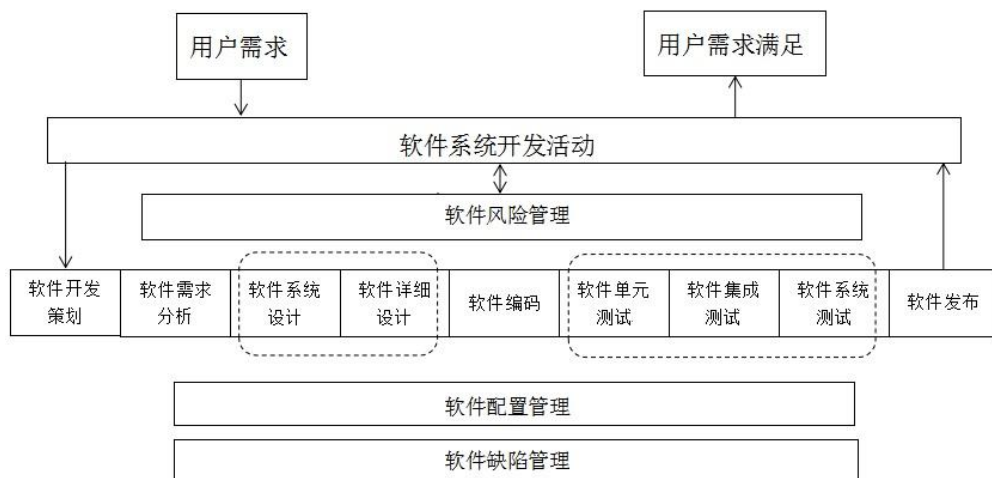


图 1 软件开发过程活动

软件开发过程的主要活动说明如下：

(1) 软件需求分析是对来自用户、法规及标准、风险等各方面需求进行分析、抽象及概括。从功能和性能、用户交互界面、报警提示、输入输出、与外部系统接口、数据定义及数据库、信息安全等主要方面对需求进行详细描述，形成软件需求规范。需求规范所包含的内容应充分、明确、完整、可追溯。需求在开发过程中通常会有更新，更新履历应与变更内容保持一致，描述完整并可追溯。

(2) 软件设计是在软件需求分析基础上，制定软件设计方案，形成软件设计规范，通常包括系统设计和详细设计两大部分。系统设计主要为软件系统总体结构的构建，从总体上对软件结构、接口以及全局数据、信息安全等进行详尽说明。详细设计则描述包括算法详细说明在内的每个模块实现细节，为后续软件编码提供直接的依据。

(3) 软件编码是将详细设计文件中各单元实现过程的描述转换为基于某种程序设计语言实现的代码。软件编码须遵循相应的编码规范要求，以保证代码质量满足安全有效的要求。

(4) 软件测试是保证软件质量的关键环节之一。软件测试目的是发现产品中存在的软件缺陷。缺陷对软件来说是必然的，越早发现，纠正成本也越低。为了尽早发现缺陷，有

效进行软件测试是必要的。按开发过程的实施先后，软件测试可分为单元测试、集成测试、系统测试。单元测试是对软件各单元部分进行的测试，通常采用白盒测试；集成测试是对各软件项（由若干软件单元组成，即软件模块）进行的测试，通常采用白盒测试、黑盒测试、灰盒测试相结合的方式；系统测试是对软件系统（由若干软件项组成）进行的测试，通常采用黑盒测试。系统测试从测试内容又可分为功能测试、性能测试、并发测试、压力测试、接口测试、内存测试、兼容性测试、用户界面测试、安装卸载测试、安全测试等。用户测试是指预期用户在真实或模拟使用场景下对软件系统进行测试，采用黑盒测试。软件测试用例需覆盖软件需求，满足可追溯性要求。测试记录必须真实、规范、完整、可追溯。软件测试是软件质量保证的基本措施，也是软件验证、软件确认的重要方式。

（5）软件维护过程适用于软件发布后的增强类软件更新，包括软件更新需求评估、软件更新策划、软件更新实施、软件验证、软件确认、软件发布、用户告知等活动。

（6）软件风险管理过程主要包括软件风险分析、评价、控制、剩余风险综合评价等活动，基于医疗器械风险管理过程予以实施，应按照 GB/T 42062-2022《医疗器械 风险管理对医疗器械的应用》的要求进行风险管理活动。软件安全性级别基于软件风险程度分为轻微、中等、严重三个级别[1]，

其中轻微级别指软件不可能产生伤害，中等级别指软件可能直接或间接产生轻微（不严重）伤害，严重级别指软件可能直接或间接产生严重伤害或导致死亡。软件安全性级别的确立是独立软件的基本要求，可结合软件的预期用途、使用场景、核心功能、软件风险等级进行综合判定[1]。

（7）软件配置管理过程包括软件配置项识别、更改控制、配置状态记录等活动。应综合考虑软件产品特点、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。软件版本命名规则应明确字段的位数、范围、含义，字段含义应明确且无歧义无矛盾，涵盖自行开发软件、现成软件、网络安全的全部软件更新类型，并能够区分重大、轻微软件更新的全部类型[1]，通常包括重大增强类软件更新、轻微增强类软件更新、纠正类软件更新、软件构建（若适用）。应基于软件版本命名规则进行软件版本控制，可使用配置管理工具或常用办公软件予以实施。应保证软件更新的版本变更符合软件版本命名规则要求。软件用户界面应体现软件发布版本和软件完整版本信息。

（8）软件缺陷管理过程适用于发布前和发布后纠正类软件更新，包括软件缺陷分析评估、软件缺陷修复、软件回归测试等活动，软件缺陷管理可通过项目管理软件、集成开发工具软件、常用办公软件等适宜工具予以实施。软件在开发过程中通常会产生缺陷，在软件生命周期中缺陷管理是保证

软件产品质量的重要环节之一。纠正类更新实施后须对软件进行回归测试，回归测试是指用于确定软件更新没有产生不良影响且未引入风险不可接受的新缺陷的软件测试。回归测试需根据软件更新的类型、内容和程度，开展与之相适宜的单元测试、集成测试、系统测试、用户测试、第三方测试等测试活动。缺陷管理记录应包括缺陷内容、原因分析、影响范围分析、解决方案、方案验证、回归测试等内容，记录需完整、充分、有效。检查时可通过调取缺陷管理相关记录予以核实。

软件开发过程、软件维护过程是前后关系，软件风险管理过程、软件配置管理过程、软件缺陷管理过程贯穿于软件开发过程、软件维护过程。

软件生存周期过程需开展可追溯性分析活动。软件可追溯性分析是指追踪软件需求、软件设计、源代码、软件测试、软件风险管理之间的关系，涵盖现成软件和网络安全，分析已识别关系的正确性、一致性、完整性。软件可追溯性分析也是软件生存周期过程的重要过程之一，同样贯穿于软件开发过程、软件维护过程，可使用追溯性分析工具或常用办公软件予以实施。

（二）软件开发过程模型

根据产品需求、风险特点、开发目标、开发资源等要素，企业可根据需要选择适宜的开发模型和实践方法。每种模型

都会涉及图 1 中软件开发过程的相应阶段活动，会产生相应的文件及记录，这些文件和记录应满足可追溯性要求，满足质量管理体系的设计开发控制、软件生存周期控制、文件控制、记录控制等相关文件要求。

软件开发应基于适宜的开发模型进行，通常软件开发过程模型包括瀑布模型、增量模型、快速原型模型、螺旋模型、统一软件开发过程模型、基于组件的开发模型、敏捷开发等。软件开发可以根据实际需要，基于一种或多种模型来实施软件开发。

主要开发过程模型简要说明如下：

(1) 瀑布模型是一种线性的开发模型，前一阶段是后一阶段的基础，具有不可回溯特点。优点是模型简单易理解，各阶段要求清晰，需求明确，实施相对容易。缺点是对开发过程中的变更不易调整，较难应对。

(2) 增量模型是把待开发的软件系统模块化，将每个模块作为一个增量组件，通过递增式的过程，分批次地分析、设计、编码和测试这些组件。最大特点是将待开发的软件系统模块化和组件化，它有以下优点：基于软件系统模块化分批次提交软件，使用户可及时了解软件项目进展；以组件为单位进行开发降低了软件开发的开发风险；开发顺序较为灵活。其缺点是待开发的软件系统需满足可被模块化的要求。

(3)快速原型模型是快速建立一个能反映用户主要需求的原型系统，通过用户试用来了了解目标系统。采用此模型可以加速开发过程，节省开发成本。其目的是通过原型获知用户的真正需求，一旦需求确定，原型将会被抛弃。

(4)螺旋模型是一种基于风险的大型软件项目开发的过程模型，是将瀑布模型和快速原型模型两者相结合，加入了风险分析后所形成的模型。其优点是将风险分析扩展到各个阶段中，大幅降低开发风险。其缺点是模型的控制管理复杂，可操作性不强，对项目管理人员和开发人员要求相对较高。

(5)统一软件开发过程模型是一种面向对象软件开发模型。它解决了螺旋模型的可操作性问题，采用迭代和增量递进的开发方法，并以用例驱动为特点，集成了多个软件开发模型的特点。基于统一软件开发过程模型所构建的系统，是由软件组件建造而成的。这些软件组件定义了明确的接口，相互连接成整个系统。软件架构包括了系统中最为重要的静态和动态特征，架构优先开发的原则是此模型至关重要的特征。

(6)基于组件的开发模型使用现成组件和系统框架进行开发，使用的现成组件已经被实际应用反复检验，其可靠性相对新组件高很多。此模型充分体现了软件复用的思想，降低了开发成本和风险，并加快了产品开发。在实际开发中经常使用。

(7)敏捷开发过程是传统方法在开发时间上经常无法满足的情况下产生的，是一种以人为中心，迭代、渐进的软件工程方法，强调快捷、小文档、轻量级。相对传统的开发模型，它更强调软件开发过程中各种变化的必然性，通过团队成员之间充分的交流与沟通，以及合理的机制来有效地响应变化。它在一定程度对解决软件开发中的不确定问题有一定的效果。在敏捷开发过程中，一个软件项目被分解成若干子项目，每个子项目的输出成果都经过测试，软件始终处在可使用评价状态。敏捷模型包括很多实践方法，比如极限编程、自适应软件开发、动态系统开发方法、特征驱动方法、自适应软件开发、统一流程、精益方法等。

(三) 独立软件描述及生产信息

(1) 产品描述信息

至少应包括独立软件的基本信息（软件标识、安全性级别、结构功能、物理拓扑、运行环境、注册历史）、实现过程（开发概述、风险管理、需求规范、生存周期、验证与确认、可追溯性分析、缺陷管理、更新历史）、核心功能等。

(2) 产品生产信息

根据交付方式不同，软件交付物的生产工艺流程也会有不同要求。生产工艺流程图如下图 2 所示，包含了物理交付及网络交付两种方式。



图 2 软件交付物生产工艺流程

五、网络安全要求

医疗器械网络安全是指保持医疗器械相关数据的保密性、完整性和可得性。对于含以下一种及以上功能的独立软件，应满足网络安全相关要求[2]：

（1）具备电子数据交换功能的软件，电子数据交换包括基于网络、存储媒介的单向、双向数据传输，其中存储媒介包括但不限于光盘、移动硬盘和 U 盘；

（2）具备远程访问与控制的软件，远程访问与控制包括基于网络的实时、非实时的访问与控制，其中网络包括无线、有线网络；

（3）具备用户访问的软件，用户（如医务人员、患者、维护人员等）访问包括基于软件用户界面、电子接口的人机交互方式。

对于网络安全适用的独立软件，企业应在产品全生命周期过程中持续关注网络安全问题，包括产品的设计开发、生产、发布、部署和维护。检查时应涵盖质量管理体系相关要求和独立软件产品特点来保证产品的网络安全，包括上市前

和上市后的相关要求，如风险管理、设计开发、网络安全维护及用户告知等要求，保证产品的安全性和有效性。

医疗器械相关数据包括标明生理、心理健康状况的私人数据（又称个人数据、敏感数据，指可用于人员身份识别的相关信息）、涉及患者隐私信息的健康数据。数据的交换方式为网络 and 存储媒介。采用网络的场合，需要考虑网络相关要求（如接口、带宽等），数据传输协议需考虑是否为标准协议（即业内公认标准所规范的协议），远程控制需考虑是否为实时控制。采用存储媒介的场合，需考虑数据储存格式是否为标准格式（即业内公认标准所规范的格式）。并结合医疗器械产品特性考虑其网络安全问题。

用户访问控制机制应与产品特性相适应。数据在网络传输或数据交换过程中应保证保密性和完整性，同时平衡可得性的要求。

此外，需要考虑包括系统软件和支持软件在内的现成软件的网络安全问题。

六、独立软件监管法规及技术标准

医疗器械软件标准根据监管用途，通常可分为管理类标准、过程类标准、产品类标准。标准、规范及指南对于软件产品风险把握、检查尺度统一、检查效率提高、企业质量管理体系水平提升有着重要影响。独立软件主要相关标准、规范及指南性文件汇总如下：

（一）软件相关通用标准

GB/T 31167-2023 《信息安全技术 云计算服务安全指南》

GB/T 31168-2023 《信息安全技术 云计算服务安全能力要求》

GB/T 42062-2022 《医疗器械 风险管理对医疗器械的应用》

GB/T 25000.1-2021 《系统与软件工程 系统与软件质量要求和评价（SQuaRE） 第 1 部分：SQuaRE 指南》

YY/T 0664-2020 《医疗器械软件 软件生存周期过程》

YY/T 1681-2019 《医疗器械唯一标识系统基础术语》

YY/T 1630-2018 《医疗器械唯一标识基本要求》

GB/T 25000.12-2017 《系统与软件工程 系统与软件质量要求和评价（SQuaRE） 第 12 部分：数据质量模型》

GB/T 35278-2017 《信息安全技术 移动终端安全保护技术要求》

YY/T 0287-2017 《医疗器械 质量管理体系 用于法规的要求》

GB/T 25000.10-2016 《系统与软件工程 系统与软件质量要求和评价（SQuaRE） 第 10 部分：系统与软件质量模型》

GB/T 25000.51-2016 《系统与软件工程 系统与软件质量要求和评价（SQuaRE） 第 51 部分：就绪可用软件产品（RUSP）的质量要求和测试细则》

YY/T 1406.1-2016《医疗器械软件 第 1 部分：YY/T 0316 应用于医疗器械软件的指南》

GB/T 32422-2015 《软件工程软件异常分类指南》

GB/T 29832.1-2013 《系统与软件可靠性 第 1 部分：指标体系》

GB/T 29832.2-2013 《系统与软件可靠性 第 2 部分：度量方法》

GB/T 29832.3-2013 《系统与软件可靠性 第 3 部分：测试方法》

（二）软件相关通用规范及指南性文件

人工智能辅助检测医疗器械（软件）临床评价注册审查指导原则（2023 年第 38 号）

影像超声人工智能软件（流程优化类功能）技术审评要点（2023 年第 23 号）

医疗器械网络安全注册审查指导原则（2022 年修订版）（2022 年第 7 号）

人工智能医疗器械注册审查指导原则（2022 年第 8 号）

医疗器械软件注册审查指导原则（2022 年修订版）（2022 年第 9 号）

肺结节 CT 图像辅助检测软件注册审查指导原则（2022 年第 21 号）

糖尿病视网膜病变眼底图像辅助诊断软件注册审查指导原则（2022 年第 23 号）

人工智能医用软件产品分类界定指导原则（2021 年第 47 号）

医用软件通用名称命名指导原则（2021 年第 48 号）

医疗器械生产质量管理规范独立软件现场检查指导原则（药监综械管〔2020〕57 号）

深度学习辅助决策医疗器械软件审评要点（2019 年第 7 号）

医疗器械生产质量管理规范附录独立软件（2019 年 第 43 号）

医学图像存储传输软件（PACS）注册技术审查指导原则（2016 年第 27 号）

中央监护软件注册技术审查指导原则（2017 年第 198 号）

移动医疗器械注册技术审查指导原则（2017 年第 222 号）

七、独立软件现场检查要点

软件是一种容易改变且难以测试的复杂产品，因而需通过较为全面的质量管理体系来保证其质量。通常，质量管理体系系统至少包括以下几个方面：详细的计划的验证和确认方案、完善的可追溯系统、软件配置管理以及变更控制系统。

根据独立软件产品的结构组成、技术特点、预期用途，在执行《医疗器械生产质量管理规范》[3]、《医疗器械生产质量管理规范附录独立软件》[4]等文件时，建议重点关注以下内容：

（一）人员

（1）（总体要求）企业应配备与产品相适宜的软件技术管理、软件开发、测试和维护人员，上述人员应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。企业应制定适宜的人员考核与评价制度，并保存相关考核及评价记录。技术研发、生产、质量的部门负责人等主要管理人员应熟悉软件产品开发及质量控制基本要求。企业执行软件黑盒测试的人员，不应承担同一软件项的开发。用户测试人员的专业知识水平、工作技能、工作经验应与被测软件产品相适宜。

（2）（培训要求）软件开发人员的培训内容应包含软件需求规范、软件设计规范、软件编码规范、软件开发工具使用、相关国家标准等内容。软件测试人员的培训内容应包含

软件需求规范、软件测试用例、软件操作使用、软件测试工具使用、软件测试数据、相关国家标准等内容。软件维护人员的培训内容应包含软件安装、设置、配置、使用、维护、软件工具使用等内容。用户测试人员的培训内容应包含测试产品的软件需求规格书、软件使用说明书、相关软件工具使用等内容。应保存相关培训记录，记录应真实、完整、清晰、可追溯。

（二）设施及设备

（1）（设备）企业应配备与检查软件产品相适应的软件开发和测试环境，包括硬件配置、软件环境、开发测试工具、网络条件等环境资源，以及病毒防护、数据备份与恢复等保证措施。应保存对软件开发和测试环境定期验证、更新升级、病毒防护等活动的记录，确保记录与相关制度要求相一致。

（2）（设施）应确保检查产品开发所涉及的机房应有适宜的空间，应满足与计算机机房相适宜的照明、温度、湿度和通风等条件的控制要求，配备防尘、防潮、防静电等必要措施。

（三）设计开发

（1）（软件生存周期控制）企业应在软件生存周期过程控制程序文件中明确与软件产品相适宜的开发要求。程序文件应至少包含软件开发、软件风险管理、软件配置管理、软件维护、软件问题解决等过程相关内容。软件开发过程应至少涵盖软件开发策划、软件需求分析、软件设计、软件单元实现、软件集成及测试、软件系统测试、软件发布等内容。软件维护过程应至少包括软件维护计划及实施方案等内容。软件风险管理应至少包含软件风险分析、风险控制措施、措施验证及评价、软件变更的风险管理等内容。软件配置管理过程应至少包括配置标识、变更控制、配置状态报告等相关内容。软件问题解决过程应至少包括缺陷原因分析、解决方案制定、解决方案实施后的验证、缺陷管理报告及回归测试报告等相关内容。企业可结合软件产品的自身特点，选用不同软件开发模型来明确生存周期活动，应确保其相关活动可追溯。如采用敏捷方法，应明确文件与记录控制要求、敏捷开发控制要求。

（2）（软件安全性级别）软件生存周期过程质量保证活动要求应与软件安全性级别相适宜，应按照软件的预期用途、使用环境、核心功能，结合风险管理的方式，判定该产品对患者、操作者或者其他人员可能引起的危害，赋予软件安全性级别，包括轻微、中等、严重三个级别。对于最初分类为

中等或严重级别的软件，可以实施软件系统外部附加风险控制措施，并在随后为软件系统赋予新的软件安全级别。

(3) (软件风险管理) 软件风险管理活动应包含识别与软件相关的危险情况、估计及评价相关风险、控制风险、监测风险控制措施的有效性，并贯穿于软件生存周期全过程。应制定剩余风险的可接受性准则，并将医疗器械产品风险控制在可接受的水平。应识别可能促成危险情况的软件项，识别该软件项促成危险情况的以下可能原因：(a) 不正确的或不完整的功能性规范；(b) 该软件项功能性方面的软件缺陷；(c) 来自未知来源软件的失效或非预期结果；(d) 可能导致不可预知的软件运行的硬件失效或其他软件缺陷；(e) 可合理预见的误使用。

(4) (软件配置管理) 软件配置管理要求至少应规定软件版本、确定配置标识（包括源代码、技术文件、工具、现成软件、数据等）、变更控制、配置状态记录等活动要求。企业应使用适宜的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。保留上述活动记录，并满足追溯要求。

(5) (软件版本控制) 软件版本变更控制应涵盖现成软件、网络安全的全部软件更新类型。软件版本命名规则应明确字段的位数、范围、含义，各字段含义应明确且无歧义无矛盾，能够区分重大增强类变更、轻微增强类变更和纠正类变更，

保证软件更新的版本变更符合软件版本命名规则要求。应保留软件版本的变更记录。

（6）（软件可追溯性）软件可追溯性分析应建立控制程序。可使用可追溯性分析工具保证软件开发、软件更新过程满足可追溯性要求。可追溯性分析报告及相关记录应覆盖包括软件需求、软件设计、软件测试、源代码、风险管理在内的软件生存周期全过程。并确认其一致性、完整性和准确性。源代码中包含追溯信息的注释应符合软件编码规范中相关要求。

（7）（现成软件）现成软件使用或更新之前应对其进行评估和确认，并保存相关记录。现成软件使用文件应明确包括现成软件基本信息、风险管理、验证与确认、缺陷管理、可追溯性分析、软件更新、配置管理、网络安全保证等活动要求。遗留软件还应确定现有文件、上市后使用情况、用户投诉、不良事件、召回情况等评估活动要求。使用现成软件应形成记录。若使用开源软件，需遵循相应开源许可协议。

（8）（软件开发过程）软件需求应包括法规、标准、用户、产品、功能、性能、接口、用户界面、网络安全、风险、警告与提示等需求。软件需求应明确、充分，与预期用途相适宜，与软件实际实现功能相一致。软件设计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、风险等相关内容。软件设计应充分、

清晰、可追溯，描述必要的核心算法，与软件实际实现功能相一致。软件编码应依据软件设计规范实施，源代码编写与注释应符合软件编码规则文件的要求。软件编码规则文件应涵盖源代码所涉及的编程语言。软件验证应确定源代码审核、静态分析、动态分析、单元测试、集成测试、系统测试、评审等活动要求，涵盖功能测试、性能测试、接口测试、现成软件、网络安全等部分的验证要求，并保存相关记录。白盒测试应确定语句、判定、条件、路径等测试覆盖率要求，并与软件安全性级别相适宜。单元测试、集成测试、系统测试应依据相应测试计划实施测试范围和活动，涵盖现成软件、网络安全的测试要求，确定缺陷管理、风险管理、可追溯性分析、评审等活动要求，并形成相应软件测试记录、缺陷管理记录、测试报告以及评审记录，应适时更新。软件测试用例的描述应充分具体、具有可操作性，覆盖主要功能和已识别的软件风险项；标准测试数据或工具应经过有效验证。软件确认应确定用户测试、临床评价、风险管理、标识、评审等活动要求，并保存相关记录。应保证软件满足用户需求和预期目的，且确保软件已知剩余缺陷的风险均可接受。用户测试应依据用户测试计划在真实使用或模拟使用环境下实施确认的范围和活动，应确定缺陷管理、风险管理、可追溯性分析、评审等活动要求，并形成用户测试记录、测试报告以及评审记录并经批准，应适时更新。

(9) (软件更新) 软件更新文件应涵盖现成软件、网络安全的变更控制要求，确定软件更新请求评估、更新策划、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，应适时更新。软件版本变更应与软件更新内容相匹配。验证与确认应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。软件缺陷管理应形成文件，确定软件缺陷的输入、分析评估、修复、回归测试、风险管理、配置管理、评审及关闭等活动要求，形成软件缺陷管理报告并评审。使用适宜的缺陷管理工具以保证软件质量，并贯穿于软件生存周期全过程。回归测试、缺陷管理及评审记录内容应充分。

(四) 采购

现成软件是指生产企业未进行或无法证明进行了完整生存周期控制的软件。现成软件采购应形成文件，根据现成软件的类型、使用方式、对产品质量影响程度，确定分类管理、质量控制、供应商审核等活动要求。

外包软件是指生产企业委托第三方开发、仅进行部分生存周期控制的软件。若使用外包软件，应与供应商签订外包软件质量协议，明确外包软件需求分析、设计开发文件交付、交付形式、知识产权归属、验收方式与准则、更新维护等要

求及双方质量责任承担要求。若使用云计算服务，应基于云计算的服务资质、服务协议、技术需求等因素选择服务商，云服务商作为医疗器械服务供应商，企业应与云服务商签订云计算服务协议，明确网络安全保证、患者数据与隐私保护等责任承担要求。

（五）生产管理

软件发布文件应确定软件的发布功能、发布流程、软件产品文件创建、软件产品与文件归档备份、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，确保软件发布的可重复性。

企业应建立软件交付物的生产作业指导书。软件交付内容一般包括软件安装程序、授权文件、外部软件环境安装程序、用户使用说明等文件。交付手段可分为通过物理存储媒介（以下简称物理交付）以及通过网络下载（以下简称网络交付）两种方式。物理交付方式应明确交付用物理存储媒介种类、物理交付物制作流程、交付物校验、软件制作工具使用、软件版本标识与标记等内容，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，应明确网络交付方式种类、网络交付物的制作流程、校验、软件上传工具使用、网络上传路径、操作人员权限、网络安全等内容，确定软件产品标记、许可授权、网络安全保证等

要求，网络交付页面的产品信息应符合相应规定。生产过程中采用的计算机软件对产品质量有影响的，应进行验证或者确认。

软件产品均应保留交付物生产记录，并满足可追溯的要求。企业应制定交付物的生产作业指导书。交付物的生产记录应与相应的生产作业指导书保持一致。生产记录应包含生产编号、光盘或 U 盘等物理存储媒介的批号/序列号（仅适用物理交付）、软件产品名称及型号、完整版本号、校验信息、生产日期、数量、主要设备、操作人员等内容。

（六）质量控制

应确保软件产品检验规程符合产品技术要求，若适用，软件产品检验规程应明确强制性标准检验要求。交付软件均应有检验记录，并满足可追溯的要求。检验记录至少应包括进货检验和成品检验的检验记录、检验报告或者证书、交付软件的系统测试报告等。

软件产品放行文件应明确产品放行条件及审核、批准要求。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，并保存相关记录。

（七）销售和售后服务

软件部署文件应确定交付、安装、设置、配置、用户培训等活动要求，并保存相关记录。

软件停运文件应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，并保存相关记录。

参考文献

[1] 国家药品监督管理局医疗器械技术审评中心. 医疗器械软件注册审查指导原则（2022 年修订版）（2022 年第 9 号）[Z]，2022.3

[2] 国家药品监督管理局医疗器械技术审评中心. 医疗器械网络安全注册审查指导原则（2022 年修订版）（2022 年第 7 号）[Z]，2022.3

[3]原国家食品药品监督管理总局.医疗器械生产质量管理规范（2014 年第 64 号公告）[Z]，2014.12

[4]国家药品监督管理局.医疗器械生产质量管理规范附录独立软件（2019 年第 43 号通告）[Z]，2019.7

此页为文件最后页