ICS 11.040.01
CCS C 30

YY

中华人民共和国医药行业标准

YY/T 1406—2026
代替 YY/T 1406.1—2016

医疗器械软件　GB/T 42062应用于医疗器械软件的指南

Medical device software—Guidance on the application of GB/T 42062 to medical device software

2026-03-09发布　　2027-03-01实施

国家药品监督管理局　　发布

目　　次

前　言

本文件按照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。

本文件代替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》，与YY/T 1406.1—2016相比，除结构调整和编辑性改动外，主要技术变化如下：

——用YY/T 0664—2020及内容代替YY/T 0664—2008及内容；

——用GB/T 42062—2022及内容代替YY/T 0316—2016及内容；

——将“总则”更改为“范围”和“规范性引用文件”（见第1章和第2章，2016年版的第1章）；

——更改了适用范围（见第1章，2016年版的1.1）；

——将术语“安全相关软件”更改为“安全有关软件”（见3.3，2016年版的2.3）；

——将“风险管理通用要求”更改为“风险管理系统通用要求”（见第4章，2016年版的第3章）；

——将“包含软件的安全的系统的特征”更改为“包含软件的安全的系统的特性”（见4.1.4，2016年版的3.1.4）；

——将“人员资格”更改为“人员能力”（见4.3，2016年版的3.3）；

——将“编程经验和意向”更改为“编程经验和意识”（见4.3.3，2016年版的3.3.3）；

——将“软件开发计划（根据YY/T 0664—2008）的风险相关主题”更改为“软件开发计划（根据YY/T 0664）风险相关的特定主题”（见4.4.3，2016年版的3.4.3）；

——将“医疗器械预期用途和与安全有关特征的识别”更改为“预期用途和可合理预见的误使用”（见5.2，2016年版的4.2），将“总则”更改为“预期用途”（见5.2.1，2016年版的4.2.1），增加了条标题“可合理预见的误使用”（见5.2.2）；

——增加了“与安全有关的特性的识别”（见5.3）；

——将条标题“危险（源）识别”更改为“危险和危险情况的识别”（见5.4，2016年版的4.3）；

——将“估计每个危险情况的风险”更改为“风险估计”（见5.4，2016年版的4.3）；

——增加了按伤害的概率和严重度进行风险估计的内容（见5.5.3）；

——删除了“降低风险”条款（见2016年版的6.1）；

——将“用设计方法取得固有安全”更改为“通过设计和制造获得固有安全”，并增加相关内容（见7.1.1.2，2016年版的6.2.1.2）；

——将“安全信息”更改为“安全信息和用户培训”，并增加相关内容（见7.1.1.4，2016年版的6.2.1.4）；

——将“风险控制措施和软件结构性设计”更改为“风险控制措施和软件体系结构设计”（见7.1.2.2，2016年版的6.2.2.2）；

——将“防护性措施细节”更改为“防护措施细节”（见7.1.2.3，2016年版的6.2.2.3）；

——将“软件异常的风险控制措施”更改为“软件反常的风险控制措施”（见7.1.2.5，2016年版的6.2.2.5）；

——将“风险/受益分析”更改为“受益-风险分析”（见7.4，2016年版的6.5）；

——将“综合剩余风险的可接受性评价”更改为“综合剩余风险评价”（见第8章，2016年版的第7章）；

——将“风险管理报告”更改为“风险管理评审”（见第9章，2016年版的第8章）；

——更改了“生产和生产后信息”（见第10章，2016年版第9章），将其拆分为“总则”（见10.1）、“信息

收集”(见10.2)、“信息评审”(见10.3)和“措施”(见10.4)四部分。

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。

本文件由国家药品监督管理局提出。

本文件由全国医疗器械质量管理和通用要求标准化技术委员会(SAC/TC 221)归口。

本文件起草单位:北京国医械华光认证有限公司、中国食品药品检定研究院、东软医疗系统股份有限公司、上海市医疗器械检验研究院、清华大学、山东省医疗器械和药品包装检验研究院、深圳迈瑞生物医疗电子股份有限公司、上海联影医疗科技股份有限公司、深圳华大智造科技股份有限公司、上海西门子医疗器械有限公司、航卫通用电气医疗系统有限公司、北京透彻未来科技有限公司。

本文件主要起草人:刘荣敏、孙业、郑佳、邵玉波、李冲、马锐兵、刘重生、岳小伟、张克、何燕德、李容、颜妙丽、卢智、韩强、王美英、常佳、王婷婷、戎澄。

本文件及其所代替文件的历次版本发布情况为:

——2016年首次发布为YY/T 1406.1—2016;

——本次为第一次修订。

引　言

软件通常是医疗器械不可或缺的组成部分。建立包含软件的医疗器械的安全和有效性，需要知晓软件的预期用途，同时要证明软件的实现满足这些预期用途且不引起任何不可接受的风险。

软件本身不是危险，但软件可促成危险情况，理解这一点很重要。宜以系统的视角考虑软件，软件的风险管理不能脱离系统孤立地进行。

复杂的软件设计可能涉及复杂的事件序列，这些序列可能促成危险情况。软件风险管理的任务主要包含识别那些能导致危险情况的事件序列，以及在这些事件序列中能在哪些位置中断序列，以防止伤害的发生或降低其发生的概率。

注1：附录A提供了软件相关危险、危险情况等定义的讨论及事件序列分析的示例。

促成危险情况的软件事件序列可分为两类：

a）　事件序列表现为软件对输入的不可预见的响应（软件规范中的错误）；

b）　事件序列是由编码错误引起的（软件实现中的错误）。

由于正确地规范和实现复杂系统的难度以及完整验证复杂系统的难度，所以这些分类对软件来说是特有的。

注2：附录B提供了导致危险的软件原因的示例。

因为很难估计会促成危险情况的软件反常的概率，并且因为软件在使用中不会因为损耗而随机失效，所以软件方面的风险分析宜关注可能导致危险情况的潜在软件功能和软件反常的识别——而不是估计概率。软件反常引发的风险大多数情况下仅需要评价伤害的严重度。

风险管理通常是有挑战性的，当涉及软件时更是如此。本文件条款包含了关于软件特性的额外的细节，这为从软件的视角理解GB/T 42062—2022提供了指南。GB/T 42062—2022和YY/T 0664—2020的内容为本文件提供了基础。

注3：附录C提供了需要在风险管理活动（针对GB/T 42062—2022的条款）和软件生存周期（针对YY/T 0664—2020的条款）中避免的与软件有关的潜在隐患。

注4：附录D提供了软件生存周期过程与风险管理过程之间的关系的信息。

本文件方框中的文本内容直接引用自GB/T 42062—2022标准，在文本的前面写明“GB/T 42062—2022原文”。此外，部分章条的标题直接使用GB/T 42062—2022相应条款的标题，条款的内容不构成要求，即使标题名称含有要求二字。

本文件借鉴IEC/TR 80002-1:2009[7]的结构和内容，并根据GB/T 42062—2022和YY/T 0664—2020的要求进行调整。此外还添加了与最新风险控制技术及风险管理实践有关的示例，以及其他内容。

本文件在医疗器械/系统中包含软件时供需要实施风险管理的风险管理从业者和需要理解如何满足GB/T 42062中阐述的风险管理要求的软件工程师使用。

本文件不涉及已由现有标准或规划中的标准所覆盖的领域，如报警、可用性工程、网络。

不预期将本文件作为法规检查或认证评定活动的依据。

本文件中“宜”用来表示在满足要求的若干可能中推荐特别适合的一种，并未提及或排斥其他的可能性，或者用来表示某种做法更好但不是必需的要求。“宜”不应理解为要求。

本文件的结构：

a）　本文件遵循了GB/T 42062—2022的结构，并为与软件有关的风险管理活动提供了指南；

b）　由于软件生存周期中风险管理活动的迭代特性，在提供的信息中存在一些有意的冗余。

医疗器械软件　GB/T 42062应用于医疗器械软件的指南

1　范围

本文件提供了将GB/T 42062—2022中包含的要求应用于YY/T 0664—2020中所指的医疗器械软件(独立软件和软件组件)的指南,本文件不增加或改变GB/T 42062—2022或YY/T 0664—2020的要求。

本文件适用于YY/T 0664—2020中所指的医疗器械软件。本文件还适用于需要实施安全风险管理过程的医疗保健环境中的所有软件,而无论其是否被归类为医疗器械。

本文件不适用于:

——生产或质量管理体系软件;

——软件开发工具。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;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。

GB/T 42062—2022　医疗器械　风险管理对医疗器械的应用

YY/T 0664—2020　医疗器械软件　软件生存周期过程

3　术语和定义

GB/T 42062—2022和YY/T 0664—2020界定的以及下列术语和定义适用于本文件。

3.1

多样性　diversity

一种冗余的形式,其中冗余要素使用不同的(多样的)组件、技术或方法以降低共同原因导致所有要素同时失效的概率。

3.2

冗余　redundancy

提供多个组件或机制来完成同样的功能,使得一个或多个组件或机制的失效不会妨碍功能的执行。

3.3

安全有关软件　safety-related software

能够促成危险情况的软件,或用于实施风险控制措施的软件。