ICS 35.240.80
CCS C30

中 华 人 民 共 和 国 国 家 标 准

GB/T XXXX.1—××××

健康软件 第 1 部分：产品安全的通用要求

Health software part1:General requirements for product safety

(IEC 82304-1:2016,MOD)

(征求意见稿)

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上

××××－××－××发布　　××××－××－××实施

国家市场监督管理总局
国家标准化管理委员会　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。

本文件修改采用IEC 82304-1:2016。

本文件与IEC 82304-1:2016的技术差异及其原因如下：

——用修改采用国际标准的YY/T 0664-2020 代替IEC 62304:2006+A1：2015，以适应我国的技术条件。

本文件与IEC 82304-1:2016的编辑性差异如下：

——用“GB 9706或YY 9706系列”代替资料性引用的“IEC60601/IEC80601系列”；

——用我国标准GB 4793系列代替IEC 61010系列；

——用我国标准GB 9706.1-2020代替国际标准IEC 60601-1:2005/AMD1:2012。

——用IEC Guide 63代替原标准中风险术语的来源。

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。

本文件由全国医用电器标准化技术委员会（SAC/TC10）归口。

本文件主要起草单位：北京怡和嘉业医疗科技股份有限公司、上海市医疗器械检验研究院、国家药品监督管理局医疗器械技术审评中心、中国食品药品检定研究院、腾讯医疗健康(深圳)有限公司。

本文件主要起草人：

健康软件 第 1 部分：产品安全的通用要求

1 范围

1.1 目的

本文件适用于健康软件产品的安全和网络安全，主要关注对制造商的要求。健康软件产品设计运行于通用计算平台，预期无需特定硬件即可上市。

1.2 应用领域

本文件涵盖整个生存周期，包括健康软件产品的设计、开发、安装，确认，维护和处理。

在每个参考标准中，术语“医疗器械”或“医疗器械软件”在适当时由术语“健康软件”或“健康软件产品”代替。

如果使用术语“患者”，无论是在本文件中还是在参考标准中，它指的是使用健康软件对其健康有益的人员。

本文件不适用于预期作为健康用途而设计的特定硬件的一部分的健康软件。具体而言，本文件不适用于：

a) GB 9706或YY 9706系列涵盖的医用电气设备或系统；

b) GB 4793系列涵盖的体外诊断设备；或

c) ISO 14708系列覆盖的植入式设备。

注：本文件也适用于旨在与移动计算平台结合使用的健康软件产品（例如医疗应用程序，健康应用程序）。

1.3 符合性

通过检查本文件要求的所有文档来确定是否符合本文件。

制造商对合规性进行评估并记录。健康软件产品如需符合监管要求，则可能需要进行外部评估。

如果本文件规范性地引用了以安全或网络安全为重点的其他标准的部分或条款，制造商可使用替代方法证明符合本文件的要求。如果这些替代方法的过程结果（包括可追溯性）明显等同并且剩余风险仍然可接受，则可使用这些替代方法。

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。

YY/T 0664-2020 医疗器械软件 软件生存周期过程（IEC 62304:2015,MOD）

3 术语和定义

下列术语和定义适用于本文件。

3.1

随附文件 accompanying document

随健康软件所带的文件，其内容包含了为责任方或使用者提供的信息，特别是关于安全和网络安全。

[来源：GB 9706.1-2020，3.4，有修改]

3.2

反常 anomaly

与基于需求规范、设计文件和标准等预期，或人的认知与经验相偏离的任何情况。

注：反常可能但不局限在健康软件或适用文档的评审，测试，分析，编译/编辑或使用过程中发现。

[来源：IEEE 1044:1993，3.1]

3.3

伤害 harm

对人健康的损伤或损害，或对财产或环境的损害。

[来源：ISO/IEC Guide63：2019，3.1]

3.4

危险 hazard

可能导致伤害的潜在根源。

注：伤害的潜在来源包括违反安全和降低有效性。

[来源：ISO/IEC guide 63：2019，3.2，有修改]

3.5

危险情况 hazardous situation

人员，财产或环境暴露于一种或多种危险中的情形。

[来源：ISO/IEC Guide 63:2019，3.3]

3.6

***健康软件 health software**

预期专门用于管理，维持或改善个人健康或提供护理的软件。

注1：健康软件完全包括医疗器械独立软件（参见A.1中的基本原理）。

注2：本文件的范围是指旨在在通用计算平台上运行的健康软件的子集。

3.7

健康软件产品 health software product

健康软件和随附文件的组合。

3.8

预期用途 intended use

预期目的 intended purpose

按照制造商提供的规范、说明书和资料，对产品、过程和服务的预期使用。

[来源：ISO 14971：2007,2.5]

3.9

IT网络 IT-network

信息技术网络 information technology network

由通信节点和传输链路组成的一个或多个系统，在两个或多个指定的通信节点之间提供物理连接或无线传输。

注：本文件中IT网络的范围是由责任方根据IT网络中的健康软件的位置和IT网络的确定用途来确定的。它能包括不是设计上预期用于医疗保健设置的IT基础设施、家庭健康或普通计算组件或系统。参见7.2.3.2 。

[来源：IEC 61907：2009，3.1.1，有修改]

3.10

制造商 manufacturer

负责设计、开发、包装、或标记健康软件产品或在健康软件产品上市之前或使用之前对其进行编译的自然人或法人,无论这些操作是否由该自然人或法人进行还是由某第三方代表自然人或法人进行。

注1：关于标记的定义，参见YY 0287-2017,3.8。

注2：“开发人员”或“开发组织”是健康信息技术背景下常用的术语，而不是制造商。

3.11

剩余风险 residual risk

实施风险控制措施后还存在的风险。

[来源：ISO/IEC Guide 63：2019，3.9]

3.12

责任方 responsible organization

对健康软件产品的使用和正确运行负有责任的实体。

注：举例来说，负有责任的实体可以是一家医院、某个医疗服务提供者或者某个远程医疗机构。

[来源： GB9706.1-2020，3.101，有修改]

3.13

风险 risk

伤害发生的概率和该伤害严重度的组合。

注：发生的概率包括暴露于危害处境以及避免或限制损害的可能性。

[来源：ISO/IEC Guide 63：2019，3.10，有修改]

3.14

风险分析 risk analysis

系统性地使用可获得的信息以识别危险和估计风险。

[来源：ISO/IEC Guide 63 ：2019，3.11]

3.15

风险评定 risk assessment

包括风险分析和风险评价的全过程。

[来源：GB/T 20002.4—2015，3.11，有修改]

3.16

风险控制 risk control

做出决策并实施措施，以便降低风险或将风险维持在规定水平的过程。

[来源：ISO/IEC Guide 63：2019，3.12]

3.17

风险评价 risk evaluation

将已估计的风险和给定的风险准则进行比较，以确定风险可接受性的过程。

[来源：ISO/IEC Guide 63：2019，3.14]

3.18

风险管理 risk management

用以风险分析、评价、控制和监视工作的管理方针、程序及其实践的系统运用。

[来源：ISO/IEC Guide63：2019，3.15]

3.19

安全 safety

免除了不可接受的风险的状态。

[来源：ISO/IEC Guide63：2019，3.16]

3.20

网络安全 security

保护信息和数据，让未经授权的人员或系统无法读取或修改它们，并且不会拒绝授权人员或系统访问它们。

[来源：ISO 12207：2008,4.39]

3.21

软件维护 software maintenance

出于下列一个或多个原因，对发布后用于预期用途的健康软件产品进行修改：

a) 纠正型，如修复错误；

b) 适应型，如适应新的硬件或软件平台；

c) 完善型，如执行新需求；

d) 预防型，如让产品易于维护。

注： 参见 ISO/IEC 14764：2006。

3.22

用户 user

与健康软件产品交互的人员。

注：通常情况下，不将用户视为责任方，但消费类的健康软件产品除外。 例如：个人健康应用，或非专业人员使用的产品。

3.23

确认 validation

通过提供客观证据对特定的预期用途或应用要求已得到满足的认定。

注1：确认所需的客观证据是试验结果或其他形式的确定结果，如变换方法进行计算或文件评审。

注2：“已确认”用于表明相应的状态。

注3：确认的使用条件可以是真实的，也可以是模拟的。

［来源：ISO 9000：2015,3.8.13］

3.24

验证 verification

通过提供客观证据，对规定要求已得到满足的认定。

注1： 验证所需的客观证据可以是检验结果或其他形式的确定结果，如变换方法进行计算或文件评审。 注2：为验证所进行的活动有时被称为鉴定过程；

注3：“已验证”一词用于表明相应的状态。

［来源：ISO/IEC Guide 63：2019，3.19］

4 *健康软件产品要求

4.1 通用要求和初始风险评定

制造商应确定并记录：

a) 健康软件产品的预期用途，包括预期的用户概况和预期的操作环境；

b) 健康软件产品的安全和（或）网络安全相关的特征，危险的识别和相关风险的估计。如适用，包括可以配置和（或）支持与其他产品接口的健康软件产品的情况；

c) 对不可接受的预估风险采取风险控制措施的必要性。

注1：第4.1条并未要求风险管理有如 YY 0316所规范的那样正式与完备，然而，执行该流程的初始步骤被认为是良好的实践。

注2：风险控制措施可以是硬件、独立软件系统，医疗护理流程或其他方式。

注3：有关网络安全漏洞的信息来源包括官方的公开报告，以及供应商的发布信息，例如操作系统和第三方软件供应商的发布信息。

4.2 健康软件产品使用需求

制造商应确定并记录：

a) 针对预期用途的需求；

b) 接口需求，包括适用的用户界面需求；

注1：与作为健康软件产品系统需求的一部分用户界面规范相比，用户界面需求不描述技术（实现）需求，他们描述了技术需求的目的。

示例：在急诊室中，显示信息可在 3 米的距离正常读取。

注2：IEC 62366-1:2015 提供了建立用户界面需求的过程。

c) 对使用共同硬件资源的其他软件的非预期影响的抵抗能力或敏感性的需求；

d) 涉及授权使用、个人身份验证、健康数据完整性和真实性以及防止恶意意图等领域的隐私和网络安全需求；

注3：有关网络安全方面的更多信息，参见 第7.2.3.1条 和 IEC TR 80001-2-2（网络安全功能列表）。

e) 随附文件的需求，如使用说明（见第7.2.2条）；

f) 支持需求：

1) 对以前版本的更新，包括保持数据完整性和与以前版本的兼容性；

2) 更新后回滚到以前的版本；

3) 及时的网络安全安装补丁和更新；

4) 确保安装完整性的软件分发机制；

5） 数据的停用、永久删除、传输和/或保留。

g） 来自适用法规的需求，包括受保护信息的规则。

注4：在某些情况下，数据保护法规（如 2016 年修订的欧洲数据保护指令 95/46/EC）要求公民保持对个人数据的控制，例如删除或导出数据。2018 年 5 月 25 日的欧洲《通用数据保护条例（2016/679） 》将取代欧洲数据保护指令 95/46/EC。

4.3 健康软件产品使用需求的验证

制造商应验证健康软件产品的使用需求：

a)使用需求被定义为系统需求的输入并形成文档；

b)使制造商能满足规定的使用需求；

应记录验证的结果。

4.4 更新健康软件产品的使用需求

适当时，制造商应确保健康软件产品使用需求的更新，例如：作为对健康软件产品使用需求验证（见第4.3条）或确认的结果。

4.5 系统需求

制造商应制定并记录健康软件产品的系统需求。这些需求应包括预期用途的功能，并在适用时包括：

a） 互操作性；

b） 本地化和语言支持；

c） 基于第 4.1条的初始风险评定，在系统层面，对健康软件产品实施的风险控制措施；

d） 用户接口规范；

e） 对软件和硬件平台的需求，以使健康软件产品在预期负载下运行预期功能并具有所需的性能水平；

f） 允许在正常使用过程中检测、识别、记录、计时和采取行动的网络安全妥协的特性；

g） 对软件产品基本功能予以保护的特性，即使软件的网络安全已受到破坏；

h） 由经过身份验证的特权用户保留和恢复产品配置的方法。

健康软件产品系统需求应满足健康软件产品使用需求（见第4.2条）。

注1：网址 http://www.himss.org/library/interoperability-standards/what-is-interoperability 提供了互操作性的信息来源。

注2：用户接口的技术需求可能包括显示颜色、字体大小、或者控件的位置。

注3：典型的软件平台包括但不限于：操作系统、设备驱动程序、软件库和其他应用程序。

注4：YY/T 0664-2020,5.2.1的软件系统需求与健康软件产品系统需求之间不是一定存在差异。

4.6 系统需求的验证

制造商应验证系统需求：

a） 互不矛盾；

b） 用避免歧义的术语表达；

c） 用条目的方式陈述，这些条目能够建立试验标准和性能测试以决定试验标准是否被达到；和

d） 能唯一识别。

应记录验证结果。

4.7 更新健康软件产品的系统需求

制造商应确保健康软件产品的系统需求在适当的时候更新，如，由于健康软件产品使用需 求的修改，或由于系统需求验证，或由于应用YY/T 0664-2020 第5.2条（软件需求分析）而进行更新。

5 *健康软件-软件生存周期过程

第4.5条中确立的健康软件产品的系统需求，应作为健康软件产品生存周期过程的首要设计输入。

除本文件的其他要求外，YY/T 0664-2020的第4.2条、第4.3条、第5章、第6章、第7章，第8章和第9章的要求应适用于健康软件。

YY/T 0664-2020规范性地引用了YY 0316。制造商可能无法为健康软件的每个组成部分遵循 YY 0316中规定的所有过程步骤这点已得到证实，例如专有组件、非医疗护理的子系统和遗留软件。在这种情况下，制造商应考虑剩余风险，对不能接受的风险进行风险控制。

6 *健康软件产品确认

6.1 确认计划

制造商应制定一份确认计划，解决第4.2条中规定的所有健康软件产品使用需求。

在确认计划里，制造商应：

a) 确定确认范围和相应的确认活动；

b) 确定可能限制确认活动可行性的约束；

c) 选择合适的确认方法，输入信息和相关的可接受准则，以便确认成功；

d) 确定支持确认所需的支持系统或服务，如操作环境，包括硬件和软件平台；

e) 指定确认人员所需的资格，如果需要培训，则应在开始确认之前完成培训；

f) 应保证确认团队与设计团队的适当独立性。

注1：约束条件包括：技术、可行性、成本、时间、是否存在确认执行者或合格人员、合同约束、任务的关键性等。

注2：确认方法包括：检验、分析、类比/类似、论证、模拟、同行评审、测试或认证。相关信息：参考标准和其他出版物，如兼容性标准，监管机构指导文件和临床文献。

6.2 实施确认

一旦出现以下情况，制造商应确定确认准备就绪：

a) 确认计划已制定；

b) 确认团队已经具备了相应的资质人员；和

c) 在适当情况下，已完成第 5 章所要求的健康软件产品经确认部分的开发生存周期阶段。

确认团队应根据第6.1条的确认计划在预期的运营环境中执行确认活动。如果认为有必要偏离确认计划， 则应在确认报告中证明其合理性。

当在确认过程中发现健康软件产品存在反常时，应根据YY/T 0664-2020第9章通过问题解决 流程处理这些问题。如果此问题解决流程导致健康软件产品的修改，则应根据修改的程度范围，对受影响部分重复执行确认。

6.3 确认报告

确认团队应根据确认情况制定健康软件产品的确认报告。

确认报告应提供以下证据：

a) 确认结果可追溯至健康软件使用需求，作为输入；

b) 健康软件产品符合第 4.2条 中规定的使用需求；和

c) 健康软件产品的剩余风险保持可被接受。

确认报告应记录确认条件和确认活动的结果。如果在确认期间，在健康软件产品中发现了反常，则 这些反常应列在确认报告中。

确认报告应列出确认团队的成员（姓名，所属机构，职能）。

确认报告应包括确认结果的摘要，以及根据使用需求确认健康软件产品是否适用于预期用途的结论。

7 健康软件产品标识和随附文件

7.1 *标识

健康软件产品应标识制造商的名称或商标，产品名称或类型参考号，以及唯一的版本标识符，例如修订级别，发布日期。

注1：在一些监管区域，器械唯一标识（UDI）是强制性的。

用户在使用健康软件时，应能够识别健康软件产品。

注2：在开始页面或登录屏幕中包含标识被认为是一种良好做法。

7.2 随附文件

7.2.1 概述

制造商应为健康软件提供随附文件，以允许用户和（或）责任方按预期实施和使用健康软件产品。

随附文件应包括：

a) 制造商的名称和联系信息，包括网站；

b) 健康软件产品标识（7.1）；

c) 健康软件产品的版本标识符，例如修订级别或发布日期，用于识别其适用的健康软件产品；

d) 随附文件的版本标识符，如修订级别或发布日期；

e) 使用说明书（7.2.2）；

f) 技术说明书（7.2.3）。

随附文件可包括软件发布说明和典型安装环境的说明。

随附文件应规定预期用户或责任方所需的特殊技能、培训和知识，对可使用健康软件产品的 地点或环境的限制，以及（如适用）系统接口、软件平台和工具以及硬件要求或限制。

随附文件的提供应符合拟使用文件的人员的教育、培训和特殊需要的水平。

注：以电子形式提供随附文件可提高可用性。当以电子方式提供时，监管机构可以指定随附文件或其部分的特 定格式。

7.2.2 使用说明书

7.2.2.1 概述

使用说明书应记录正确操作健康软件产品所需的内容，包括适当的安装说明。如适用，使用说明书应规定对使用健康软件产品的IT网络的限制（7.2.3.2）。

注：使用说明书适用于用户和责任方，仅包含对用户或责任方有用的信息。其他细节可包含在技术说明书中（见7.2.3）。

7.2.2.2 健康软件描述

使用说明书应包括：

a) 制造商规定的健康软件产品的预期用途；

b) 健康软件产品的简介，包括健康软件产品的基本功能；

c) 使用健康软件的操作网络安全选项；

d) 使用健康软件产品的已知的技术问题、限制、免责声明或禁忌症。

7.2.2.3 安全和/或网络安全的警告和注意事项

使用说明书应列出与使用健康软件产品有关的安全和（或）网络安全的警告和注意事项，并在非不言自明时对其进行说明或扩充。

安全和（或）网络安全的一般警告和注意事项宜放在使用说明书的特殊可识别的章节。对特定的指令或动作适用安全或网络安全的警告或通知，应在它适用的指令之前。

7.2.2.4 安装

使用说明书应包含：

a) 声明是由用户安装，还是应由制造商完成或在制造商协助下安装，或由授权人员完成；

b) 预期执行健康软件的软件平台和硬件平台的系统要求；

c) 在安装时设置健康软件的可选的网络安全选项；

d) 对其他应用程序的全部关键依赖；

e) 配置要求；

f) 系统接口要求（必需和可选）；

g） 支持的软件平台的细节；和
h） 安装说明或参考安装说明的位置。

7.2.2.5 启动流程

使用说明书应包含用户使健康软件开始运行的必要信息。

7.2.2.6 关闭流程

使用说明书应包含用户使健康软件结束运行的必要信息。

7.2.2.7 操作说明

使用说明书应包含操作健康软件所需的信息。这应包括对控制，显示和信号功能以及操作顺序 的说明。

使用说明书应说明数字，符号，警告声明和缩写的含义。

7.2.2.8 消息

使用说明书应列出生成的系统消息，错误消息和故障消息，除非这些消息是不言自明的。

注：可以分组识别这些消息。

该列表应包括对消息的解释，包括重要原因， 以及用户可能采取的行动（如果有的话）， 以解决消息所指示的情况。

7.2.2.9 健康软件停用和处理

使用说明书应包含用户或责任方安全地停用和处理健康软件所需的信息。这应酌情包括保护与网络安全和隐私有关的个人和健康数据。

注：监管机构可以在处理个人和健康相关数据时指定要求。

7.2.2.10 技术说明书参考

使用说明书应包含技术说明书（7.2.3）或可以找到技术说明书的参考。

7.2.3 技术说明书

7.2.3.1 概述

技术说明书应提供安全可靠的操作、运输和存储所必需的信息，以及安装和准备使用健康软件 所需的措施或条件。应包括：

a） 用于执行健康软件的软件和硬件平台的系统要求；
b） 支持的软件平台的详细信息；
c） 运输和储存含有健康软件的媒介的允许环境条件；
d） 健康软件的特征，包括显示值的范围，准确度和精确度，或者可以找到它们的指示；
e） 特殊安装要求或限制；
f） 维护要求，例如要检查和可能清除的日志文件，数据库维护和存储媒介的更改；
g） 责任方可用的健康软件产品可配置的网络安全技术选项，此类网络安全可能包 括：
1） 配置选项，例如最少的网络端口列表和所需的计算机服务；
2） 软件选项，例如打开加密设置，更改默认登录凭据；
3） 操作选项，例如审计和日志记录管理设置。
h） 当检测到未能保持网络安全时，应对软件所做的操作进行描述。描述应包括对患者护理，数据 或临床工作流程的影响。

注：由于健康软件通常运行在多个硬件和软件平台，在某些情况下，对典型特征和约束的文件化以及成功实施的描述，可以提供有效的帮助。

制造商应在用户和（或）责任方的技术说明书中提供有关如何处理硬件和软件平台变更的说明（例如，使用防病毒/防火墙软件、系统库、固件和其他软件的补丁/更新），以及如何选择适当的平台设置来支持网络安全目标和网络安全能力。

7.2.3.2 *预期在 IT 网络中使用的健康软件

IT网络的范围可能包括预期未明确用于支持医疗保健环境的IT基础设施或系统。见第3.9条。

如果健康软件预期在不受健康软件制造商控制的IT网络中使用，则制造商应作为技术说明书的一部分提供此用途所需的说明，包括但不限于以下：

a) 健康软件实现其目的所需的 IT 网络的特征和配置；
b) 健康软件实现其目的所需的 IT 网络技术规范，包括网络安全规范和防恶意软件或类似软件；
c) 使用 IT 网络在健康软件与其他软件或系统之间的预期信息流。

制造商应在技术说明书中包括由于IT网络未能在使用该IT网络时提供健康软件所需的特性和服务而导致的危害处境列表。

在技术说明书中，制造商应通知责任方：

a) 在 IT 网络上执行健康软件可能会导致患者，用户或第三方以前未识别出的风险；
b) 建议责任方识别，分析，评估和控制这些风险；
c) 对 IT 网络的变更可能会引入新的风险并需要额外的分析；并且
d) IT 网络的变更包括：
    1) IT 网络配置的变更；
    2) 向IT网络添加项目（硬件和（或）软件平台或软件应用程序）；
    3) 从IT网络中删除项目；
    4) 更新IT网络上的硬件和（或）软件平台或软件应用程序；和
    5) 升级IT网络上的硬件和（或）软件平台或软件应用程序。

注：IEC 80001-1提供了对健康软件制造商，其他信息技术提供商和责任方的要求，以解决IT网络修改的风险。

8 健康软件产品的上市后活动

8.1 概述

根据第1章， 本文件涵盖了健康软件的整个生存周期。在其生存周期内，健康软件可能会进行软件 维护，最终会停用和处理。第4.2条规定了在使产品可供使用之前实施和确认的使用需求；这些要求包括停用和处理健康软件产品。当本文件用于合规目的时，仅与产品设计和开发相关的上市后方面的要求适用。

8.2 软件维护

如果制造商确定软件维护是相关或必要的，例如，由于检测到的错误可能会对安全和（或）网络安全产生影响，制造商应根据本文件制定健康软件产品的修改（见第5章）。

注1：维护还可包括随附文件的变更，例如：关于健康软件的运行平台。

注2：当软件维护是因为检测到的错误会影响安全和（或）网络安全时，在此种情况下需要考虑法规要求。

8.3 重新确认

制造商应确保考虑到修改的程度，重新确认受软件维护影响的健康软件产品部分的有效性。制造商应相应更新确认计划。

制造商应确保修改后的健康软件版本适用于声称支持的全部硬件和软件平台。

8.4 健康软件产品的上市后沟通

制造商应向用户和责任方通知制造商已经了解的健康软件产品的网络安全漏洞以及影响健康软件产品使用的法规要求变更。

对于软件维护，制造商应向用户和责任方提供有关健康软件产品更新版本的信息，并在适当情况下提供以下信息：

a) 新功能；
b) 纠正的错误或故障；
c) 对修改后的软件的安全和（或）网络安全的影响；
d) 更新健康软件标识（7.1）；

e） 随附文件的更新（7.2） 。

用户或责任方是否安装修改版本的健康软件的决定宜基于修改的安全和（或）网络安全影响。 如果修改后的健康软件产品对健康软件的安全和（或）网络安全产生积极影响，制造商可建议用户和责任方在短期内更换其版本。

8.5 健康软件产品的停用和处理

用户或责任方应能够在其使用寿命结束时安全地停用和处理健康软件产品，包括在适当情况下保护 与网络安全和隐私相关的个人和健康相关数据。健康软件应提供与第4.2条中规定的使用需求一致的功能。

附 录 A
（资料性附录）
本文件要求的理由说明

A.1 概述

健康软件由其制造商专门用于健康目的。这包括预期帮助诊断、治疗或监测患者，或帮助补偿或减轻疾病，伤害或残疾的应用。

在本文件开发的早期阶段，使用以下术语来指示软件作为（硬件）医疗器械的一部分（“医疗器械软件”）和本身即为医疗器械的软件（软件医疗器械）。各自的定义是：医疗器械软件：专门用于嵌入到物理医疗器械中的软件；以及软件医疗器械：本身即是医疗器械的软件。这两个子类别的组合被定义为：医疗软件：预期专门用于嵌入到物理医疗器械或旨在作为软件医疗器械的软件。

健康软件，如第3.6条中所定义：“预期专门用于管理，维持或改善个人健康，或提供护理”，完全包括“医疗软件”，但更广泛。医疗软件与术语医疗器械密切相关，医疗软件是一个监管定义，其因管辖区而异。就本文件而言，健康软件一词被认为更合适。在更广泛的范围内，本文件允许对与健康相关的软件产品的安全、网络安全和性能采取共同的方法，无论它们是否作为医疗器械进行管理。

国际医疗器械监管机构论坛（IMDRF）已发布文件SaMD WG/N10 FINAL：“医疗器械独立软件（SaMD）：关键定义”。如果健康软件具有医疗用途且不预期运行于特定硬件，则它归于医疗器械独立软件。

请注意，本文件仅针对健康软件产品提供要求，即作为独立产品提供的健康软件。预期在特定硬件上运行的健康软件（有时也称为“嵌入式”软件）被认为是物理设备的一部分，而不是产品本身。另见A.2。

健康软件包括处理健康，健康管理和医疗保健资源管理的应用程序。表A.1给出了本文件涉及的软件产品示例。ISO/TR 17791介绍了健康软件标准的概况，识别出按现有标准覆盖健康软件存在的差距。对于独立的健康应用程序，引用安全/网络安全的标准看起来是缺失的。本文件旨在填补这一空白。

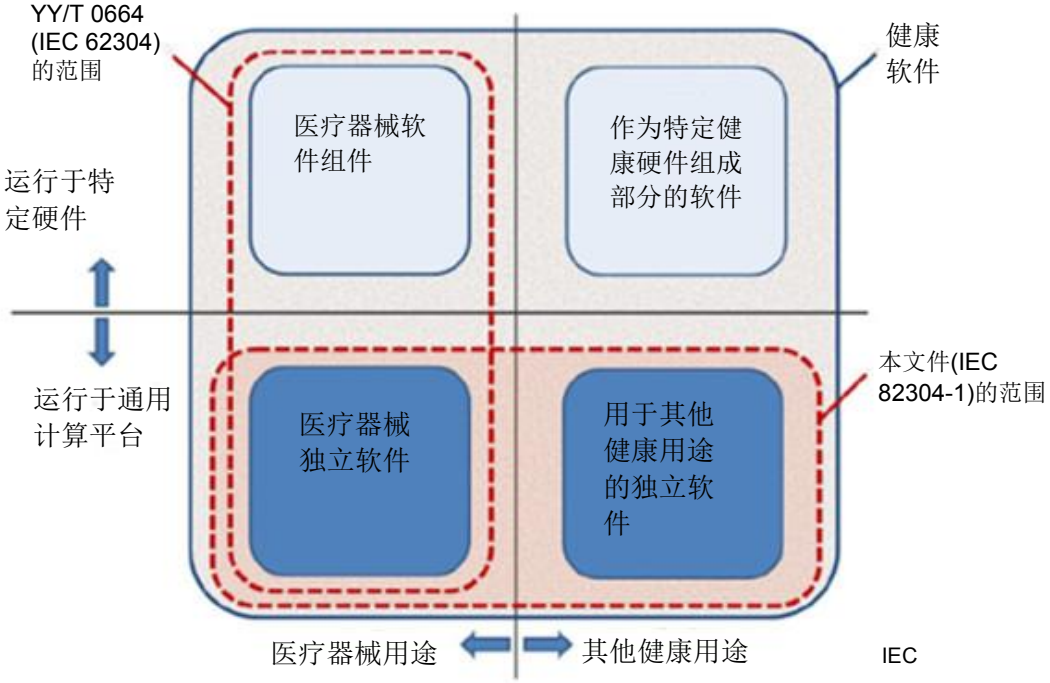
每个管辖区都必须自行决定哪些健康软件产品被认为受其医疗器械法规的约束，或者当不作为医疗器械管理时，是否适用其他法规。鼓励有意在已采纳本文件的管辖区内投放健康软件领域内的软件产品的制造商，调查哪些监管制度适用(如果有的话)。

表A.1 本文件适用范围内或不在本文件适用范围内的软件示例

在适用范围	不在适用范围
- 健康用途的纯软件产品 - 在不使用特定传感器或探测器的设备上运行的移动应用[a] - 实验室信息软件 - 放射学信息软件 - 健身中心的个人软件 - 最佳受孕时机软件 - 计算机辅助诊断软件 - 分析医学图像的软件 - 临床决策支持软件，用于辅助个人的诊断，治疗和健康管理 - 具有反馈的个人减压软件 - 用于重新确认目的的培训计划软件 - 用于刺激阿尔茨海默病患者活动的软件 - 电子健康记录系统，电子病历系统 - 医院信息系统 - 由外部组织提供的健康软件服务	- 不具备可执行性的软件，例如参考值集。 - 不解决个人健康问题的软件 - 医院账单软件 - 医院设备维护调度软件 - 流行病学研究软件 - 护士训练软件 - 医学专业人员的自学软件 - 疗养院的电子日志 在范围之外也还是软件或是其更新，旨在驱动（部分）： - 9706系列涵盖的医用电气设备或系统；（任一部分） - 4793系列涵盖的体外诊断设备（任一部分） - ISO14708 涵盖的可植入设备（任一部分） 。
[a] 智能手机或平板电脑上常见的相机或麦克风或其他特性不被视为特定的传感器或检测器。	

A.2 健康软件产品的要求

请注意，本文件仅提供作为独立产品的健康软件的要求。 图A.1显示了健康软件的应用领域及其相关标准的相应覆盖范围，即本文件和YY/T 0664-2020。



图A.1 健康软件应用领域和相关标准的范围

健康软件通常运行于各种有较大差异的平台上，平台包括硬件和软件。例如：固定或移动物理设备，或虚拟机、本地或网络或作为“云”-通过互联网托管的服务。这些平台往往超出制造商的影响和控制。因此，本文件还预期引导制造商和责任方注意必要的考虑因素、任务和文件，以充分解决可能由于使用的多样性和频繁变化的平台而导致的危害。

预期在特定硬件上运行的健康软件应被视为物理设备的一部分，有时也称为“嵌入式”软件。这种软件本身并不是一种产品。这既适用于作为医疗器械监管的产品中的软件，也适用于不作为医疗器械受监管的特定物理设备的一部分的软件。

A.3 特定条款和子条款的基本原理

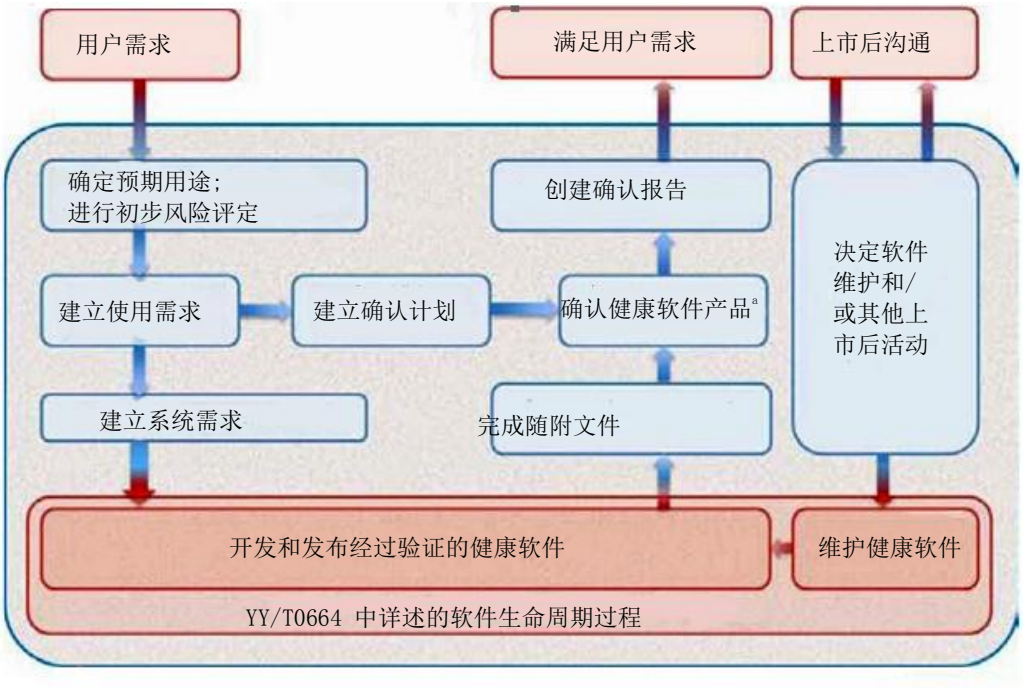
3.6-健康软件的定义

根据ISO 17791：2013，健康软件还包括-基于其基本形式-系统、软件项和软件单元（参见YY/T 0664-2020 的定义3.30,3.25和3.28），以及相关的编码系统，推理 引擎，原型和知识库。此外，它包括使用，受益或适用于卫生部门部分的软件，包括所有公共和私营 组织或企业以及消费者。

3.6中的健康软件定义与ISO 17791：2013，2.6中相同术语的定义不相冲突。

第4章-健康软件产品需求

通常的做法是根据预期用途建立产品的使用需求，并且确认最终产品的标准是基于这些客户或使用需求。定义系统需求和最终产品的确认之间的阶段是产品开发过程。这种开发过程如图A.2所示。实际过程可以遵循各种方案，例如瀑布模型或更多迭代或增量开发方案。本文件不要求或优先考虑特定的过程方案。



[a]健康软件产品：健康软件加随附文档

图A.2　IEC82304-1 健康软件产品流程

用户需求是开发过程的输入，并流经一系列解释这些用户需求的过程。一旦建立了系统需求，就可以启动YY/T 0664-2020中描述的过程。这些过程导致经过确认的健康软件与文档一起发布。根据此文档，随后最终确定了随附文件，使健康软件成为真正的健康软件产品，可以接受有效保护。

对于健康软件产品的确认，本文件要求基于使用需求的确认计划；见第4.2条和第4.3条。成功确认后，可以认为健康软件产品可满足用户需求。由制造商决定是否将健康软件产品投放市场；除了成功的确认之外的其他考虑可以影响该决定。

在上市后阶段，制造商可能会收到或积极收集有关健康软件产品的反馈。根据这些信息或其他考虑因素，可以对上市后活动做出决定。这些活动可能包括软件维护，必须遵循与初始开发相同的过程 （如果适用）。其他上市后活动可以是与用户或监管的沟通，例如涉及网络安全漏洞的沟通。

与健康软件相关的危害可能源于可用性问题。在确定使用需求时，建议参考IEC 62366-1：2015了解可用性工程流程。

YY/T 0664-2020 处理医疗器械软件的生存周期过程，涵盖整个软件开发方案。 YY/T 0664-2020旨在参考其他系统安全标准。本文件(IEC 82304-1)涵盖整个产品生存周期，并在适用的情况下规范性地参考 YY/T 0664-2020。

第5章-健康软件-软件生存周期过程

本文件包含基于风险/收益的方法。本文件的用户需要建立、维护和应用风险管理流程，作为合规性的一部分。 YY/T 0664-2020 中记录了该要求以及软件生存周期过程的其他要求。这些要求同样适用于健康软件，并通过引用规范性地包含在本文件中。

第6章-健康软件产品确认

健康软件开发生存周期模型的最后阶段是健康软件产品确认。确认过程的目的是提供客观证 据，证明健康软件产品在其预期的操作环境中符合健康软件产品使用需求（见4.2）。健康软件产品确 认旨在确保构建正确的产品。确认对于健康软件产品很重要，因为可能会发生只能通过确认发现的功能 之间的意外交互。

健康软件产品确认可包括对大量数据、高负载或压力、人因、性能、配置兼容性、数据、环境和系统完整性、故障测试、文档、安全和网络安全的测试。

独立性是必需的，至少强烈建议，以避免利益冲突并且因为设计者的假设不宜影响或限制健康软件产 品确认的范围。独立程度的例子包括：

a) 独立的人员；

b) 独立的管理；

c) 独立的组织。

7.1-标识

软件可以轻松更新或升级，有时无需用户参与。重要的是，可以识别所使用的健康软件的特定版本。术语“版本标识符”适用于此特定健康软件版本，而不是健康软件的单个副本。用于每个版本的标识符宜具有独特性，以区分使用中的健康软件版本与之前版本的健康软件。

7.2.3.2-旨在用于IT网络的健康软件

本文件建议参考IEC 80001-1和IEC 80001-2-2，以获取更多信息和有用的指导，尽管IEC 80001当前版本的范围仅限于医疗器械和（或）医疗器械软件。

当阅读IEC 80001-1和IEC 80001-2-2用于本文件时，其中的术语“医疗器械”可以理解为“健康软件产品”；“医疗器械制造商”称为“健康软件产品制造商”。

参 考 文 献

[1] GB 4793(所有部分)测量、控制和实验室用电气设备的安全要求

[2] GB 9706(所有部分) 医用电气设备

[3] GB 9706.1-2020 医用电气设备 第1部分：基本安全和基本性能的通用要求

[4] GB/T 20002.4-2015 标准中特定内容的起草 第4部分：标准中涉及安全的内容

[5] IEC 61907:2009 Communication network dependability engineering

[6] IEC 62366-1:2015 Medical devices - Part 1: Application of usability engineering to medical devices

[7] IEC 80001-1:2021 Application of risk management for IT-networks incorporating medical devices - Part 1: Roles, responsibilities and activities

[8] IEC/TR 80001-2-2:2012 Application of risk management for IT-networks incorporating medical devices - Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls

[9] ISO/IEC 12207:2008 Systems and software engineering -- Software life cycle processes

[10] ISO/IEC 14764:2006 Software Engineering -- Software Life Cycle Processes --Maintenance

[11] ISO/IEC Guide63:2012 Guide to the development and inclusion of safety aspects in international standards for medical devices

[12] ISO 9000:2015 Quality management systems - Fundamentals and vocabulary

[13] ISO 13485:2016 Medical devices - Quality management systems - Requirements for regulatory purposes

[14] ISO 14708(all parts)Implants for surgery-Active implantable medical devices

[15] ISO 14971:2007 Medical devices — Application of risk management to medical devices

[16] ISO/TR 17791:2013 Health informatics — Guidance on standards for enabling safety in health software

[17] IEEE 1044:1993 Classification for software anomalies

[18] WHO:1946 Preamble to the Constitution of the World Health Organization as adopted by the international Heath Conference,New York,19-22 June,1946;Signed on 22 July 1946 by the representatives of 61 States (Official Records of the World Health Organization,no.2,p.100)and entered into force on 7 April 1948

[19] IMDRF/SaMD WG/N10FINAL:2013 Software as a Medical Device (SaMD):Key Definitions (http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-131209-smad-key-definitions-140901.pdf)

[20] HIMSS/NEMA HN 1-2013 Manufacturer Disclosure Statement for Medical Device Security(https://www.nema.org/standsrds/Pages/Manufacturer-Disclosure-statement-for-Medical-Device-Security.aspx).