ICS 35.240.80
CCS C 30

中华人民共和国国家标准

GB/T 44585.1—2024

风险管理在接入IT网络的医疗器械中的应用 第1部分：联网医疗器械或健康软件在其实施和使用中的安全、有效性和网络安全

Application of risk management for medical device connecting IT-network—Part 1: Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software

（IEC 80001-1:2021, Application of risk management for IT-networks incorporating medical devices—Part 1: Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software, MOD）

2024-09-29 发布　　2026-04-01 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。

本文件是GB/T 44585《风险管理在接入IT网络的医疗器械中的应用》的第1部分。GB/T 44585已经发布了以下部分：

——第1部分：联网医疗器械或健康软件在其实施和使用中的安全、有效性和网络安全。

本文件修改采用IEC 80001-1:2021《包含医疗器械的IT网络的风险管理应用　第1部分：联网医疗器械或健康软件在其实施和使用中的安全、有效性和网络安全》。

本文件与IEC 80001-1:2021的技术差异及其原因如下：

——增加了“安全”“保证案例”“变更-发布管理”“风险”“风险分析”“风险估计”“风险管理”“风险控制”“风险评估”“风险评价”“关键属性”“管理员”“集成商”“健康IT”“健康IT基础设施”“健康IT系统”“健康软件”“角色”“可用性”“伤害”“社会技术生态系统”“剩余风险”“随附文档”“随附文件”“随附资料”“网络安全”“网络安全能力”“危险”“威胁”“验证”“严重度”“医疗服务提供机构”“用户”“制造商”“资产”“组件”“组织”“最高管理者”的术语和定义（见第3章）（IEC 80001-1:2021继承了ISO 81001-1:2021的术语，但ISO 81001-1:2021并未转化为我国标准，因此基于差异，增加了ISO 81001-1:2021中提及的使用在IEC 80001-1:2021的术语）；

——更改了“验证”“过程”术语的定义，与GB/T 19000—2016相统一。

本文件做了下列编辑性改动：

——将标准名称改为《风险管理在接入IT网络的医疗器械中的应用　第1部分：联网医疗器械或健康软件在其实施和使用中的安全、有效性和网络安全》；

——更改了附录B的内容表述格式。

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/TC 10）归口。

本文件起草单位：上海市医疗器械检验研究院、北京怡和嘉业医疗科技股份有限公司、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、东软医疗系统股份有限公司、深圳迈瑞生物医疗电子股份有限公司、首都医科大学宣武医院、上海交通大学医学院附属瑞金医院。

本文件主要起草人：刘重生、陈兴文、彭亮、李澍、陶华、史大鹏、费晓璐、朱立峰、陈士妹、陈蓓。

引　言

虽然数字医疗的优势已被广泛接受，但是对健康软件和健康IT系统的安全、有效性和网络安全造成的潜在意外和不利影响也越来越明显。当今先进的健康软件和健康IT系统提供了先进的决策支持，但除了患者和医疗系统的获益外，同时也增加了因软件引起的不良事件对患者和医疗机构造成伤害的可能性。医疗服务提供机构依赖安全的、有效的和具备网络安全的系统作为运营的关键因素。然而，对联网系统的实施和使用的管理不力可能会威胁到其提供医疗服务的能力。

提供健康服务的联网系统通常涉及多个软件应用程序、多种医疗设备和复杂的健康IT系统，这些系统依赖于健康IT基础设施，包括有线或无线网络、点对点连接、应用服务器和数据存储、接口引擎、安全和性能管理软件等。健康IT基础设施通常用于临床功能（例如，患者监测系统）和非临床组织功能（例如，会计、日程安排、社交网络、多媒体、文件共享）。通过健康IT基础设施连接的系统涉及小型的部门级网络，也涉及跨越多个地点的大型集成基础设施，以及由第三方运营提供的基于云的服务。本文件中的要求则适用于将风险管理应用于包括健康IT系统和/或健康IT基础设施在内的系统的多种利益相关方。

管理健康软件和健康IT系统（包括医疗器械）的安全、有效性和网络安全，需要采取全面和协调的方法来优化这三种属性，许多组织和角色参与了健康软件和健康IT系统的整个生存周期（见图1）。本文件则是覆盖了该生存周期的实施阶段及临床使用阶段，而本文件的其他关联文件将从不同的技术特性的层面在此阶段的应用提出指南或要求，如无线网络的指南、通用的实施指南、分布式报警系统的指南等。

本文件有助于组织在可行的情况下使用或调整现有的工作实践和流程、人员和工具来满足本文件的要求。例如，如果组织有现有的风险管理流程，则使用或调整该流程来支持安全、有效性和网络安全这三个关键属性。定义要求以便对其进行评估，并因此支持组织验证和证明对本文件的符合程度。

GB/T 44585《风险管理在接入IT网络的医疗器械中的应用》规定了各利益相关方对于联网医疗器械或健康软件在其生存周期中如何应用风险管理的一般要求，拟由一个部分组成。

——第1部分:联网医疗器械或健康软件在其实施和使用中的安全、有效性和网络安全。目的在于规范在健康IT基础设施内连接健康IT系统之前、期间和之后,组织机构通过同时让适当的利益相关方参与进来的方式处理这三个关键属性应用风险管理方面的一般要求。

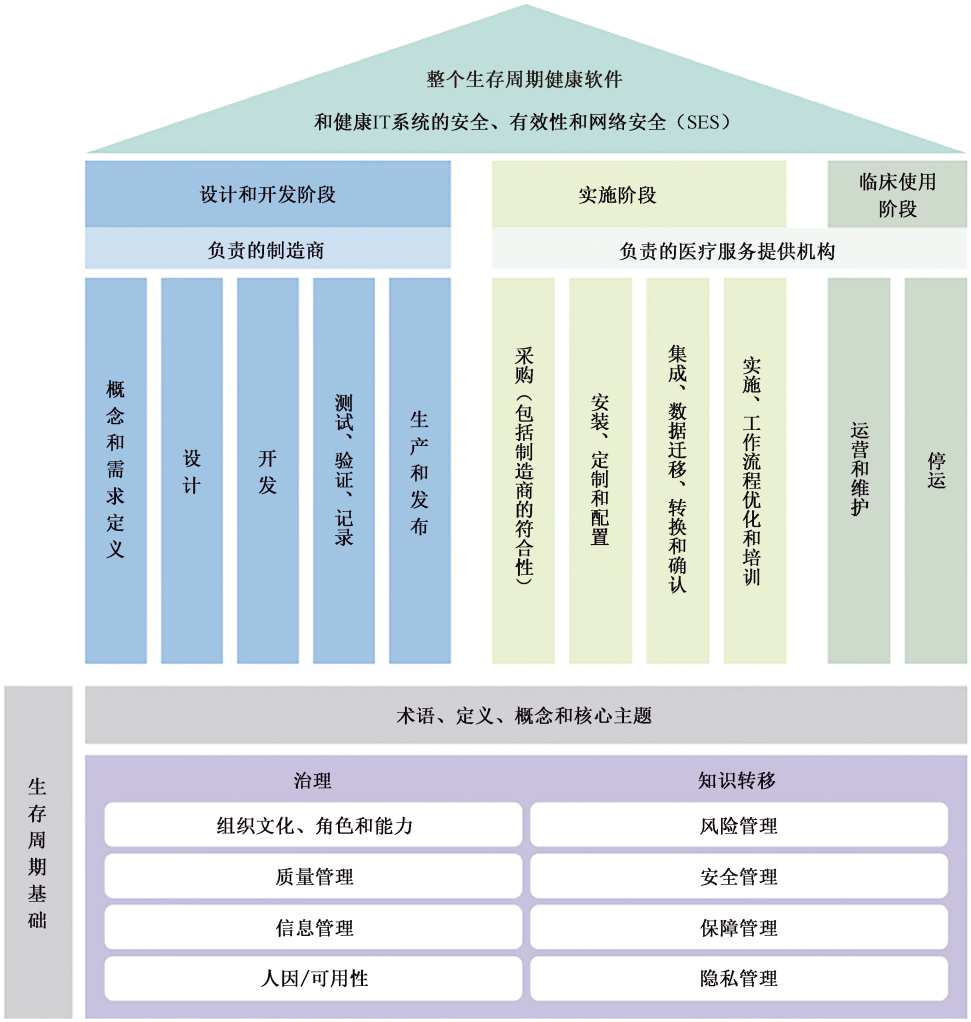

图 1　涉及健康软件和健康 IT 系统的安全、有效性和网络安全的生存周期框架

风险管理在接入IT网络的医疗器械中的应用 第1部分：联网医疗器械或健康软件在其实施和使用中的安全、有效性和网络安全

1 范围

本文件规定了在健康IT基础设施内连接健康IT系统之前、期间和之后，组织机构通过同时让适当的利益相关方参与进来的方式处理安全、有效性和网络安全这三个关键属性应用风险管理方面的一般要求。

本文件适用于联网医疗器械或健康软件在生存周期实施和使用阶段的风险管理。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

后果 consequence

某事件对目标影响的结果。

注1：后果可能是确定的，也可能是不确定的，它可能对目标产生积极或消极的直接或间接影响。

注2：后果可能是定性或定量表述。

注3：任何后果都可能通过连锁反应和累积效应升级。

[来源：GB/T 24353—2022，3.6，有修改]

3.2

医疗 healthcare

与个体或人群医疗相关的护理活动、服务、管理或用品。

注：这不仅包括为护理对象执行程序。例如，它包括在医疗健康提供框架内对有关患者、医疗状况和关系的信息的管理，还可能包括对临床知识的管理。

[来源：ISO 13940:2015，3.1.1，有修改]

3.3

事故 incident

服务的意外中断、服务质量的降低或尚未影响客户或用户服务的事件。

[来源：ISO/IEC 20000-1:2018，3.2.5]

3.4

初始风险 initial risk

在考虑任何保留的风险控制措施的情况下，风险评估出的风险。