ICS 11.040.01
CCS C 30

YY

中华人民共和国医药行业标准

YY/T 1843—2022

医用电气设备网络安全基本要求

Basic requirements of cybersecurity for medical electrical equipment

2022-05-18 发布　　2023-06-01 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。

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：上海市医疗器械检测所、国家药品监督管理局医疗器械技术审评中心、国家计算机网络应急技术处理协调中心、中国食品药品检定研究院、江苏省医疗器械检测所、苏州UL美华认证有限公司、深圳迈瑞生物医疗电子股份有限公司、东软医疗系统股份有限公司、深圳市理邦精密仪器股份有限公司、北京怡和嘉业医疗科技股份有限公司、飞利浦(中国)投资有限公司、上海西门子医疗器械有限公司、通用电气医疗系统贸易发展(上海)有限公司、美敦力(上海)管理有限公司。

本文件主要起草人：刘重生、彭亮、邢潇、王晨希、刘茹、张波、陶华、马锐兵、陈勇强、陈蓓、谌达宇、曹景泰、秦川、夏伟杰。

引　言

随着医疗应用场景的不断拓展，以及网络技术的快速发展和互联网应用的普遍化，医疗器械越来越多地进行着不同目的、不同类型的数据交换，在提高诊疗效率，提升数据分析能力的同时，也出现了诸如患者信息泄露、健康数据被篡改、未授权修改治疗参数、以勒索或其他非法目的为目标的恶意攻击或数据窃取等情况发生。

在这样的背景下，当下的医疗器械不论是单机使用，还是在个域网、局域网或广域网中使用，其网络安全能力对于医疗器械的安全性、有效性则变得至关重要。而网络安全，从广义来说，凡是涉及医用电气设备、医用电气系统及相关医疗器械软件产品的信息的保密性、完整性、可得性等相关技术和理论都是其范畴之内的。

虽然从保障网络安全的责任角度讲，在使用环境中，维系一个 IT 网络的网络安全是多方责任，但对制造商来说，有义务识别产品本身可能遇到的网络安全相关的风险并予以识别和分析，进而在设计、开发的过程中实现对应的风险控制措施。本文件则将对医用电气设备、医用电气系统或医疗器械软件产品（在本文件中，“产品”一般指医用电气设备、医用电气系统或医疗器械软件产品）的网络安全能力提出基本要求并规范了验证过程（见附录 A），以验证制造商对产品网络安全相关风险的风险控制措施的实现情况。

考虑到目前制造商在识别网络安全风险时普遍会参考 IEC/TR 80001-2-2，对于风险识别的维度，本文件中也一定程度上参考了 IEC/TR 80001-2-2，因此本文件和 IEC/TR 80001-2-2 是有一定关联性的。为了描述这种关联性，本文件列出了本文件与该文件相关条款之间的对应关系（见附录 B）。

星号（*）作为标题的第一个字符、段落或表格标题的开头，表示在附录 C 中有与该项目相关的指南或原理说明。

医用电气设备网络安全基本要求

1 * 范围

本文件规定了医用电气设备、医用电气系统及医疗器械软件的网络安全基本要求。

本文件适用于有用户访问、电子数据交换或远程控制功能的医用电气设备、医用电气系统及医疗器械软件。

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

安全性 safety

不会对人员、财产或环境造成不可接受的风险。

[来源:ISO/IEC GUIDE 51:2014,3.14,有修改]

3.2

保密性 confidentiality

信息对未授权的个人、实体或过程不可用或不泄露的特性。

[来源:GB/T 29246—2017,2.12]

3.3

恶意软件 malware

设计为恶意破坏正常功能,收集敏感数据和/或访问其他连接系统的软件。

3.4

防火墙 firewall

对经过的数据流进行解析,并实现访问控制及安全防护功能的网络安全产品。

3.5

风险 risk

伤害发生的概率和该伤害严重度的组合。

[来源:YY/T 0316—2016,2.16]

3.6

风险分析 risk analysis

系统地运用现有信息确定危险(源)和估计风险的过程。

[来源:YY/T 0316—2016, 2.17]

3.7

风险控制 risk control

作出决策并实施措施,以便降低风险或把风险维持在规定水平的过程。

[来源:YY/T 0316—2016, 2.19]