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]

3.8

风险管理　risk management

用于风险的分析、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：YY/T 0316—2016，2.22]

3.9

个人敏感数据　personal sensitive data

一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。

注 1：个人敏感数据可能包括身份证件号码、个人生物识别信息、银行账号、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、14 岁以下(含)儿童的个人信息等。

注 2：在 GB/T 35273—2020 中，被称之为个人敏感信息，由于本文件主要是对数据进行规范，因此在本文件中改写为数据。

注 3：关于个人敏感数据的判定方法和类型可参考 GB/T 35273—2020 中的附录 B。

[来源：GB/T 35273—2020，3.2，有修改]

3.10

紧急访问　emergency access

在紧急的情况(如抢救、急救)下，临床用户能够在不使用个人身份标识或未经授权的情况下对健康数据进行访问。

3.11

健康数据　health data

与身体或心理健康相关的个人敏感数据。

注 1：通常在本文件中将健康数据定义为个人敏感数据的子集。

注 2：由于目前全球规定了不同的隐私合规性法律和法规。例如，在欧洲，可能需要采取的要求和参考变更为“个人数据”和“敏感数据”，在美国，健康数据可能会更改为“受保护的健康信息(PHI)”，这需要不同国家或地区的制造商进一步考虑中国当地的法律或法规。

[来源：IEC/TR 80001-2-2：2012，3.7，有修改]

3.12

抗抵赖性　non-repudiation

证明所声称事件或行为的发生及其源头的能力。

[来源：GB/T 29246—2017，2.54，有修改]

3.13

可核查性　accountability

实体的活动可以被唯一地追溯到该实体的程度。

3.14

可得性　availability

根据授权个人、实体的要求可访问和使用的特性，即产品相关数据能以预期方式适时进行访问和使用。

[来源：GB/T 29246—2017，2.9，有修改]

3.15

敏感数据　sensitive data

敏感数据是任何可能危及产品使用和网络安全的关键安全参数，如密码、密钥、随机数生成器的种子、身份验证数据、个人敏感数据以及未授权访问可能危及产品网络安全的任何数据。

[来源：UL2900-1，3.41]

3.16

匿名化　anonymization

通过对个人敏感数据的技术处理，使得个人敏感数据主体无法被识别或者关联，且处理后的信息不能被复原的过程。

[来源：GB/T 35273—2020，3.14，有修改]

3.17

去标识化　de-identification

通过对个人敏感数据的技术处理，使其在不借助额外信息的情况下，无法识别或者关联个人敏感数据主体的过程。

注：去标识化建立在个体基础之上，保留了个体颗粒度，采用假名、加密、哈希函数等技术手段替代对个人敏感数据的标识。

[来源：GB/T 35273—2020，3.15，有修改]

3.18

设备数据　equipment data

描述设备运行状况的数据，用于监视、控制设备运行或用于设备的维护保养，本身不涉及个人敏感数据。

3.19

审计日志　audit logging

为了评审和分析以及持续监控而收集的有关信息安全事态的数据。

[来源：GB/T 25068.1—2020，3.4]

3.20

网络安全能力　security capability

基于风险管理使产品数据和/或功能具有可接受水平的保密性、完整性、可得性等网络安全特性的技术措施。

注：本文件中，为了在区分 security 和 safety 的中文，将 security 称之为网络安全，而 safety 称之为安全性。

[来源：IEC/TR 80001-2-2：2012，3.27，有修改]

3.21

网络安全能力说明　security capability description

阐明产品网络安全能力的文档，其主要目的是作为测试者对产品进行测试的依据。

注：本文件并不规定网络安全能力说明的形式，可以是一个文档，也可以是一套文档集，也可以是一个文档的一部分。

3.22

完整性　integrity

数据自创建、传输或存储以来，无未经授权的方式被更改的属性。

[来源：ISO/IEC 29167-19：2016，3.40]

3.23

信息技术网络　IT-network

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

[来源：IEC/TR 80001-2-2：2012，3.10]

3.24

医疗器械软件　medical device software

在包括在医疗器械内的已开发的软件系统，或者预期本身用作医疗器械而开发的软件系统。

[来源：YY/T 0664—2020，3.11]

3.25

医用电气设备　medical electrical equipment

ME 设备　ME equipment

具有应用部分或向患者传送或取得能量或检测这些所传送或取得能量的电气设备。这样的电气设备：

a）　与某一指定供电网有不多于一个的连接；且

b）　其制造商旨在将它用于：

1）　对患者的诊断、治疗或监护；或

2）　消除或减轻疾病、损伤或残疾。

[来源：GB 9706.1—2020，3.63]

3.26

医用电气系统　medical electrical system

ME 系统　ME system

在制造商的规定下由功能连接或使用多位插座相互连接的若干设备构成的组合，组合中至少有一个是 ME 设备。

[来源：GB 9706.1—2020，3.64]

3.27

医用信息技术网络　medical IT-network

包含至少一个医疗器械的信息技术网络。

[来源：IEC 80001-1：2010，2.16]

3.28

自动注销　automatic logoff

产品在闲置一段时间后自动登出或锁定以阻止未经授权的使用和误用。

注：自动锁定也可以理解为是一种自动注销的手段。

3.29

责任方　responsible organization

对产品的使用或保养负有责任的实体。

注 1：举例来说，这样负有责任的实体可以是一家医院、一个临床医生或一个业外人士。对家用设备来说，患者、操作者和责任方有可能是同一个人。

注 2："使用"包含了教育和培训。

[来源：GB 9706.1—2020，3.101，有修改]

3.30

真实性　authenticity

实体符合其所声称的特性。

[来源：GB/T 29246—2017，2.8，有修改]

3.31

制造商　manufacturer

以其名义制造预期可用的医疗器械并负有医疗器械设计和/或制造责任的自然人或法人，无论此医疗器械的设计和/或制造是由该自然人或法人进行或由另外的一个或多个自然人或法人代表其进行。

[来源：YY/T 0287—2017，3.10]

4 通用要求

4.1 * 网络安全能力说明

4.1.1 标识和内容

4.1.1.1 网络安全能力说明应体现其文档标识。

4.1.1.2 网络安全能力说明应能识别对应产品的标识。

4.1.1.3 网络安全能力说明应按照 4.1.4～4.1.20 的要求，根据产品的适用情况阐明网络安全能力。

4.1.1.4 网络安全能力说明中陈述的网络安全特性应是可测试或可验证的。

4.1.2 * 分类

4.1.2.1 按预期接入的网络的类型可分为预期接入专用网络、公共网络的产品。

4.1.2.2 按预期接入网络的域可以分为预期接入个域网、局域网、广域网的产品。

4.1.2.3 按连接类型可分为预期与其他信息设备单独进行有线、无线连接的产品。

注：其中有线连接可能包括了：USB、RS232 等方式，无线连接可能包括了 wifi 通讯、蓝牙通讯、私有频段的私有协议的无线通讯等方式。

4.1.2.4 按数据交换过程中的数据传输方向可以分为单向传输、双向传输。

4.1.2.5 按使用场景可分为医疗场景和非医疗场景。

注：其中医疗场景可能包括了治疗、诊断或监护等场景，非医疗场景可能包括了维护场景等。

4.1.3 产品特征描述

4.1.3.1 网络安全能力说明应按照 4.1.2 对产品进行分类。

4.1.3.2 网络安全能力说明应明确产品的预期用途。

4.1.3.3 网络安全能力说明应提供产品在其预期配置中的所有电子接口的列表，包括了：

a) 所有远程接口；

b) 所有本地接口、产品本地内部接口；

注：内部接口指的是 ME 系统中各部件之间的接口。

c) 所有无线接口；

d) 所有外部文件的输入接口；

e) 每个接口支持的所有通信协议及其用途。

4.1.3.4 * 网络安全能力说明应列明产品的软件名称和版本号，这里包括了所有第三方和包含在产品中的开源软件。

4.1.3.5 网络安全能力说明应指明产品中使用的不同配置或所支持的配置。

注 1：这里指的配置是软件、硬件配置，如：

——操作系统、系统软件或其他支持软件；

——处理器及其规模、主内存及其规模、输入输出设备；

——网络环境。

注 2：针对不同的需求，可以规定不同的配置。但是制造商需识别不同的操作系统所带来的网络安全风险。

4.1.4 存储保密性

网络安全能力说明应包含有关敏感数据的存储保密性的陈述。

4.1.5 传输保密性

网络安全能力说明应包含有关传输保密性的陈述，尤其是对敏感数据的考量。

注 1：需着重考虑当设备在公用网络进行网络数据传输过程中的敏感数据保密性策略。

注 2：有关在无线网络中传输保密性的更多信息，可参考 IEC/TR 80001-2-3:2012。

4.1.6 健康数据中的身份信息

网络安全能力说明应列出产品包含的个人敏感数据的类型，以及选取的个人敏感数据类型的依从性文件。

注 1：关于可能的类型和内容见附录 D 或 GB/T 35273—2020。

如适用，网络安全能力说明应包含数据导出时使个人敏感数据无法被识别的手段的陈述。

注 2：更多细节可参考 GB/T 37964—2019 。

4.1.7 * 用户访问控制

网络安全能力说明应包含产品用户访问控制的陈述，这包括采用的用户访问控制措施以及这种控制措施的细节。

注：这包括了远程访问，其中也包括了远程控制和用于维护的远程访问。

4.1.8 用户授权

网络安全能力说明应包含产品是否提供了用户身份验证的陈述，若提供了这种手段，则应陈述所有现有用户身份及其访问权限。

4.1.9 自动注销

网络安全能力说明应包含有关自动注销的陈述。

注：若产品部署于医疗服务提供组织（Healthcare Delivery Organization；HDO），某些场景自动注销功能会影响可得性，制造商需要考虑这样的场景下自动注销功能所带来的风险。

4.1.10 紧急访问

网络安全能力说明应包含产品是否提供了紧急访问的陈述，若提供了用于紧急访问的功能，则应陈述该功能的必要性，以及使用该功能的同时如何兼顾完整性。

4.1.11 传输完整性

网络安全能力说明应包含在传输过程中保证敏感数据完整性的策略的陈述。

注：该陈述可以包括对数据传输的路径的要求。

4.1.12 节点认证

适用时，网络安全能力说明应包含节点认证的陈述。

若设备部署在 HDO，身份验证策略宜灵活适应本地 HDO 信息技术网络的安全策略。

若产品包含了多个节点，且节点有可能被产品之外的其他节点接入，则应考虑这种情况的节点认证。

注：节点认证的方式一般包括了白名单、用户名/口令、证书等。

4.1.13 恶意软件探测与防护

网络安全能力说明应包含产品是否支持恶意软件探测与防护的陈述，这应包括安全产品的配置方式，探测到恶意软件时的处理和修复方式。

注：安全产品一般包括杀毒软件、辅助安全软件和防火墙等。

4.1.14 * 系统与应用软件固化

制造商应考虑产品的系统与应用软件固化，若需要实施固化，网络安全能力说明应包含系统与应用软件固化的措施的陈述，这样的措施用于保证仅提供与预期用途相关的资源和服务，并保证尽可能少的维护活动。

注：这样的措施的举例：

——关闭/禁用与产品预期用途无关的访问端口；

——关闭/禁用与产品预期用途无关的服务；

——关闭/禁用与产品预期用途无关的应用软件；

——限制/控制资源层的访问；

——限制/控制任务层的访问。

4.1.15 物理防护

网络安全能力说明应包含产品上的数据交换端口的物理防护的陈述。

若产品部署在 HDO，网络安全能力说明应包含产品有关物理防护的陈述。

注：哪怕该物理设备的资产不属于制造商，若存在相关的风险，也需要进行陈述。

4.1.16 抗抵赖性

网络安全能力说明应包含产品有关抗抵赖性的陈述。

4.1.17 健康数据的完整性和真实性

网络安全能力说明应包含有关保证健康数据的完整性和真实性的陈述。

4.1.18 可核查性

网络安全能力说明应包含产品有关可核查性内容及其手段的陈述。

注：对于这样的内容的举例：

——成功或失败的登录尝试；

——健康数据的访问、修改和删除；

——健康数据的导入、导出；

——安全配置的更改（如，更改用户身份验证的凭据、更改有效的用户账户列表）；

——远程访问（可能是用于产品维护或实现预期用途）；

——紧急访问。

4.1.19 数据备份与灾难恢复

网络安全能力说明应包含产品进行数据备份与灾难恢复策略的陈述。

注：其目标是为了确保医疗业务持续进行。利用第三方和操作系统的功能进行数据备份在本文件中是被认可的。这包含了系统遭灾的恢复的考量。尤其是需要存档健康数据的产品，需要考虑提供灾难恢复的策略。

4.1.20 维护性

4.1.20.1 网络安全能力说明中应包含与产品维护计划中与网络安全有关的维护内容，并明确网络安全维护的责任方。

4.1.20.2 * 第三方组件

若产品中包含了第三方组件，应在网络安全能力说明中列出第三方组件的信息。

注：第三方组件可能包括操作系统、第三方的动态链接库、第三方的应用程序等现成软件。第三方组件的信息可以

是标识、来源及版本号等。

4.1.20.3 产品的网络安全升级

网络安全能力说明应包含产品的网络安全升级的陈述。

注：这样的升级可能包括安全补丁文件的安装、安全产品的升级。

4.2 用户文档集的要求

4.2.1 标识和内容

4.2.1.1 用户文档集应体现其唯一的文档标识。

4.2.1.2 用户文档集应能识别对应产品的标识。

4.2.1.3 用户文档集中陈述的网络安全特性应是可测试或可验证的。

4.2.1.4 用户文档集应包含产品预期用途及其配置的安全注意事项的陈述。

4.2.1.5 用户文档集应包含产品预期使用场景(见 4.1.2)的陈述。

4.2.1.6 用户文档集应包含网络安全相关的产品配置和产品部署环境的要求或建议的陈述。

注：例如，对产品的物理访问控制、防火墙端口和协议、本地接口的配置选项等方面的要求。

4.2.2 管理职能

若产品部署在 HDO，用户文档集应明确用户的管理职能，尤其是 IT 管理员的责任。

注 1：考虑到 IT 管理员的职能的独立性，推荐发布单独的管理员手册，以便仅能由管理员对其保管和查看。

注 2：关于“职能”，必要时，明确的指出管理员需要完成那些工作，如管理、定制和监视系统的信息(如访问控制列表、审计日志等)，且需要让管理员清楚地了解与安全相关的功能。

注 3：即便 IT 管理员是由供应商/制造商派遣，这样的责任也要明确。

4.2.3 健康数据中的身份信息

用户文档集应按照网络安全能力说明的陈述提供如何去除健康数据中的身份信息必要的指导。

4.2.4 用户访问控制

用户文档集应包含有关用户访问控制的功能的指导。

4.2.5 用户授权

用户文档集应陈述所有现有角色及其访问权限。

4.2.6 自动注销

用户文档集应按照网络安全能力说明的陈述提供有关自动注销的参考信息。

4.2.7 紧急访问

用户文档集应陈述紧急状态下访问必要的产品功能或健康数据的指导。

4.2.8 安全产品

若安全产品可由用户安装，则用户文档集应陈述产品所兼容的安全产品，并应提供安全产品的配置指导。

4.2.9 物理防护

用户文档集应按照网络安全能力说明的陈述提供有关产品物理防护的参考信息。

4.2.10 可核查性

用户文档集应按照网络安全能力说明的陈述提供有关如何查看网络安全事件记录的指导。

4.2.11 数据备份与灾难恢复

用户文档集应按照网络安全能力说明的陈述提供产品数据备份与灾难恢复的必要的指导。

4.2.12 维护性

用户文档集应包含在网络安全能力说明中陈述的维护性相关内容的指导。

用户文档集中应陈述与产品维护计划中和网络安全有关的维护服务。

用户文档集应包括在存储设备退役之际保证敏感数据不可再被访问的指导。

注：退役的情况可能有丢弃、重新使用、转售或回收等。

4.3 网络安全能力要求

4.3.1 保密性

4.3.1.1 产品应按照网络安全能力说明所陈述的保密性特征来实现。

4.3.1.2 产品应提供该产品生成、存储、使用或传输的所有敏感数据的保密性手段。

4.3.2 健康数据中的身份信息

若产品可将个人敏感数据导出，产品应提供使其无法识别患者身份的必要的信息的手段。

注 1：这样的手段可能包括匿名化、去标识化等。

注 2：使用制造商指定的第三方工具完成上述目标也是可以接受的。

4.3.3 * 用户访问控制

产品应按照网络安全能力说明中有关用户访问控制措施的陈述来实现。

若产品预置了供操作者使用的缺省用户名和口令，应提供这样的手段，在操作者第一次访问之后被要求修改用户名或口令。

若产品部署在 HDO，应对设备、网络资源和健康数据的访问进行控制。

注：在紧急访问期间，这个要求是放宽的，见 4.3.6。

若产品使用身份验证凭据的机制来进行用户访问控制，则：

a) 产品提供的身份验证错误消息不准许枚举有效凭据。

b) 产品应满足制造商规定的凭证复杂度、不成功尝试的次数、更新频率、强度或长度的要求。

c) 产品的默认凭证应可以被修改或替代。

4.3.4 用户授权

产品应按照网络安全能力说明中有关用户授权的陈述来实现。

若产品可以基于用户角色进行配置，则产品的网络安全管理功能应不能配置给临床用户这种角色。

产品的用户角色分配宜按照最小授权的原则进行分配。

注：如果产品未实现用户访问控制措施，在本文件中则认为是授权给所有可以使用到产品的人。有些情况，如产品部署在设置了门禁的房间内，虽然被认为是降低了未授权访问的风险，但这并不在本文件的评价范围内。

4.3.5 * 自动注销

产品应按照网络安全能力说明和用户文档中有关自动注销的陈述来实现。

注 1：自动锁定也可以被认为是一种等同于自动注销的方式，但在解锁时需要重新登录。

对有用户访问控制的产品应实施闲置超时或其他适当的机制，以防止永久授权。闲置超时的间隔可由用户配置，或可基于产品对事件或动作的响应类型进行配置。

注 2：这样的配置可能包括了自动注销禁用、自动注销时间设置等。

产品宜不能使用户因自动锁定而丢失未提交的临床业务。

除非有临床需要，否则产品应不能在自动注销后的界面显示健康数据或患者信息。

4.3.6 * 紧急访问

产品应符合网络安全能力说明中有关紧急访问的陈述。

如适用，在紧急情况下，应提供可以访问健康数据的手段。紧急访问的行为应被记录并可供核查。

4.3.7 传输完整性

产品应符合网络安全能力说明中有关传输完整性的陈述。

4.3.8 节点认证

产品应符合网络安全能力说明中有关节点认证的陈述。

如适用，产品应支持通过添加、删除和/或挂起需要认证的节点名称，或添加、撤消或更新身份验证凭据来管理有效的节点。

4.3.9 恶意软件探测与防护

产品应符合网络安全能力说明中有关恶意软件探测与防护的陈述。

应保证在用户文档集中陈述的安全软件与产品的兼容性。

产品的最终交付物应不存在已知恶意软件。

4.3.10 系统与应用软件固化

产品应按照网络安全能力说明中有关系统与应用软件固化的陈述实现。

产品的最终交付物应不存在网络安全风险不可接受的已知漏洞。

4.3.11 物理防护

产品应按照网络安全能力说明中有关物理防护的陈述进行防护。

4.3.12 抗抵赖性

产品应按照网络安全能力说明中有关抗抵赖性的陈述实现。

4.3.13 健康数据的完整性和真实性

产品应按照网络安全能力说明中有关健康数据的完整性和真实性的陈述进行实现。

4.3.14 * 可核查性

产品应按照网络安全能力说明中有关可核查性的陈述实现。

产品应能够通过在设备上创建审计日志来记录和检查用户的行为，审计日志应能明确的追踪到访问网络、设备或资源的用户。

审计日志应仅由授权用户访问，且应不能被编辑或非授权的删除。制造商应制定审计日志存储策略，以保证审计日志不会非预期的丢失。

注 1：审计日志中记录的行为属性一般包括但不限于日期、时间、用户身份标识、事件。

注 2：在紧急访问期间，这个要求是被放宽的，见 4.3.6。

4.3.15 数据备份与灾难恢复

产品应按照网络安全能力说明中有关数据备份与灾难恢复的陈述进行实现。

适用时，应提供一种手段确保在系统故障或遭受损害后可以恢复存储在产品上的持久性系统设置和健康数据。

4.3.16 维护性

产品应按照网络安全能力说明和用户文档集中有关维护性的陈述来执行。

5 试验方法

5.1 通过查验产品网络安全能力说明来验证是否符合 4.1 的要求。

5.2 通过查验用户文档集来验证是否符合 4.2 的要求。

5.3 通过进行满足附录 A 要求的网络安全能力测试过程的测试，来验证产品是否符合 4.3 中陈述的要求的符合性。

附 录 A
（规范性）
网络安全能力测试过程的要求

A.1 总则

按照此测试过程进行网络安全测试的目的是有效证实产品是否符合 4.3 的要求。基于此测试过程的文档一般应包含测试计划、测试说明和测试结果（报告），但本文件并不对具体有哪些文档做出规定。这些文档不应与产品矛盾，如果有多个文档构成，那么每个文档之间也不应自相矛盾。

A.2 内容要求

测试过程中通常包含以下文档：测试计划、测试说明和测试结果（报告）。

注：本文件不对都有哪些测试文档进行要求。

A.3 测试计划的要求

测试计划的要求通常包括了以下内容，但也可以由测试者自定义。

A.3.1 通过/失败准则

测试计划应指明用于判定测试结果是否证实软件与网络安全能力说明和用户文档集的符合性准则。

A.3.2 测试环境

测试计划应规定将要进行的测试所处的软件测试环境或配置。

A.3.3 进度

测试计划应规定每个测试活动和测试里程碑的进度。

A.3.4 风险

测试计划应识别、更新并记录测试活动中存在的风险，并提供应对措施。

A.3.5 人力资源

测试计划中应明确每个测试活动所需的人力资源情况。

A.3.6 工具和环境资源

A.3.6.1 测试计划中应明确执行测试活动所需的工具。

A.3.6.2 如果使用特殊的工具和环境，测试计划中应说明选择这些工具和环境的原因以及预期的结果。

A.4 测试说明的要求

A.4.1 测试用例

对每个测试用例的说明可包括：

a) 测试目标；
b) 唯一性标识符；
c) 测试的输入数据和测试边界；
d) 实施步骤；
e) 系统的预期行为；
f) 测试用例的预期输出；
g) 结果解释的准则；
h) 用于判定测试用例的肯定或否定结果的准则。

编制的测试用例应基于一定的测试规程来进行测试。

注：本文件不会提供测试用例的模板，也不会对测试用例的模板进行要求，但 GB/T 15532—2008 提供模板的参考。

A.4.2 测试规程

A.4.2.1 测试规程可包括：
a) 测试准备；
b) 开始和执行测试所必需的动作；
c) 记录测试结果所必需的动作；
d) 停止和最终重新启动测试的条件和动作。

A.4.2.2 为提供测试的可重复性和可再现性，测试规程应足够详细。

A.4.2.3 在产品被纠正后应有一种重新测试的规程。

A.5 测试结果的要求

A.5.1 执行报告应包括测试用例结果的全部汇总。

A.5.2 执行报告应证实已按测试计划执行了所有测试用例，或对测试计划偏差进行了分析。

A.5.3 对于每个测试用例，执行报告均应包括以下内容：
a) 测试用例的标识符；
b) 测试执行日期；
c) 实施测试的人员姓名和职责；
d) 测试用例执行的结果。

注：对于发现的异常或不符合项，需考虑编写异常情况报告给相关利益方。本文件虽然不对异常报告的格式和全部内容进行要求，但若编写异常报告，异常报告需具有可追溯性。

A.6 方法

A.6.1 本文件未推荐特定的技术或方法。

A.6.2 在网络安全能力说明和 4.3 中提及的所有网络安全能力均应经测试用例测试。

A.6.3 适用时，在网络安全能力说明和 4.3 中提及的每个网络安全能力至少应经一个测试用例测试。

A.6.4 测试用例应能证实产品与用户文档集中的陈述的符合性。

A.6.5 当网络安全能力说明中引用了任何需求文档时，所涉及的内容应经测试用例测试。

A.6.6 若产品实施了系统与应用软件固化，则所有的固化措施都应经过测试用例的测试。

注：若使用漏洞扫描工具进行这样的测试，漏洞库的信息也需被记录。

A.6.7 当 4.3 的任何要求不适用时，应在测试记录中阐述不适用的理由。

附 录 B
（资料性）
本文件与其他文件的关联

表 B.1 列出了本文件与 IEC/TR 80001-2-2 相关条款的关联性。

表 B.1 与 IEC/TR 80001-2-2 的关联

本文件条标题	章条号	IEC/TR 80001-2-2 中的缩写
存储保密性	4.1.4、4.3.1	STCF
传输保密性	4.1.5、4.3.1	TXCF
健康数据中的身份信息	4.1.6、4.3.2	DIDT
用户访问控制	4.1.7、4.2.4、4.3.3	PAUT
用户授权	4.1.8、4.2.5、4.3.4	AUTH
自动注销	4.1.9、4.2.6、4.3.5	ALOF
紧急访问	4.1.10、4.2.7、4.3.6	EMRG
传输完整性	4.1.11、4.3.7	TXIG
节点认证	4.1.12、4.3.8	NAUT
恶意软件探测与防护	4.1.13、4.2.8、4.3.9	MLDP
系统与应用软件固化	4.1.14、4.3.10	SAHD
物理防护	4.1.15、4.2.9、4.3.11	PLOK
抗抵赖性	4.1.16、4.3.12	—
健康数据的完整性和真实性	4.1.17、4.3.13	IGAU
可核查性	4.1.18、4.2.10、4.3.14	AUDT
数据备份与灾难恢复	4.1.19、4.2.11、4.3.15	DTBK
维护性	4.1.20、4.2.12、4.3.16	RDMP、CSUP、MLDP
用户文档集的要求	4.2	CNFS、SGUD

附 录 C
（资料性）
特定条款的指南和原理说明

C.1 通用指南

对于制造商来说，对网络安全风险的考虑是贯穿于整个产品的生命周期的，基于本文件进行的验证同样也可以在产品生命周期的任何时间进行，但更多的情况是会发生在验收的时机。

本文件第4章由网络安全能力说明、用户文档集、网络安全能力要求构成，这些内容构成了符合性测试活动的输入。制造商需要从风险管理的角度考虑产品的网络安全能力，并按4.1的要求陈述在网络安全能力说明中。

对于与本文件相关产品的网络安全风险，可以参考YY/T 0316—2016的基础流程，对于网络安全风险，目前国际上亦有一些标准可供参考，如GB 9706.1—2020的第14章可编程医用电气系统(PEMS)、IEC 80001-1及其系列技术报告、UL2900-2-1、AAMI TIR57等标准中的相关内容。

本文件中网络安全能力说明中要求的网络安全能力则通常是为了缓解网络安全风险而实现的技术控制措施，对于其他的某些管理上的或行政上的控制措施则可能会作为某种警告性语言陈述在用户文档中。当这些风险控制措施引入到设计需求时，制造商还需要考虑是否会引入新的风险。

C.2 特定条款的指南或原理说明

以下是本文件中特定章条号的指南或原理说明，与本文件正文的章条号相对应。

条款1 范围

本文件范围的定制是基于参考ME设备、ME系统以及医疗器械软件的定义。这样的列举也是为了明确与全国医用电器标准化技术委员会(SAC/TC 10)之间的关系。本文件中的ME设备和ME系统的定义是等同于GB 9706.1的，然而考虑到医疗器械网络安全特性的通用性，在GB 9706.1中列出不适用的医疗器械(如：体外诊断设备、有源植入装置的植入部分或医用气体管道系统等)也可以参考本文件进行评测。

本文件中医疗器械软件的定义则来自YY/T 0664。在医疗器械内的已开发的软件系统是基于本文件随ME设备或ME系统共同评测的，而预期本身用作医疗器械而开发的软件则通常单独评测，但这也不排除有些情况下，需求方想要单独基于本文件评测在医疗器械内的已开发的软件系统。

值得注意的是，本条中陈述的范围排除了那些无网络安全风险的用户交互，比如那些没有用户交互界面的人机交互模式为机械交互的产品。

条款4.1 网络安全能力说明

在更多的情况下，在进行产品网络安全能力的验证时，网络安全测试的测试者需要制造商来陈述产品本身的网络安全能力作为测试需求分析的输入，因此网络安全能力说明通常由制造商进行撰写。

制造商需要陈述的网络安全能力的内容通常是基于产品进行的网络安全的风险管理活动的风险控制的技术措施，这些风险管理活动应结合产品的预期用途、使用场景及核心功能等进行分析，当产品的预期用途结合了不同的场景时，可能会产生不同的风险，如果制造商在设计产品时基于不同的场景实现了不同的网络安全能力，则制造商需要分别陈述这些网络安全能力，这也是为什么网络安全能力说明要

按照 4.1.3 的要求对产品的特征进行陈述，以帮助潜在的测试者初步了解产品。

在 4.1.4～4.1.20 中，从多个方面提出了产品可能具有的网络安全能力，制造商则需要分析产品于这些网络安全特性的适用性，适用的，则需要将实现的风险控制的技术措施在网络安全能力说明中进行陈述。对于不适用的项目，制造商仍需要陈述其不适用的理由。只有能够通过风险识别证明产品在不进行任何技术措施的情况下，产品不存在对应的不可接受的网络安全风险，条款才可能被认为是不适用的。

对于网络安全能力说明中对网络安全特性陈述的细化程度，首先需要考虑陈述的网络安全能力的可测试性，其次则要明确这次测试的时机，比如，如果测试的时机是产品上市前(Pre-Marketing)，那么列出那些只有上市后(Post-Marketing)才能实现的手段要求测试者进行验证显然是不合适的。

另外，除了 4.1.4～4.1.20 提出的要求，制造商也可以在网络安全能力说明中陈述那些本文件中没有明确提出要求但又希望宣称的已实现的网络安全能力，比如，为了防止 SQL 注入而使用正则表达式过滤掉字符中的特殊字符，为了防止拒绝服务(DoS)攻击而实现登录时需要输入验证码或限制了请求频率等手段。这样的目标是能够一定程度上来提高网络安全能力说明编写的灵活性，以便更好地适应特定的监管政策或制造商的需求。

条款 4.1.2　分类

本条的目标是为了让产品网络安全能力说明的编写者在陈述产品特征描述中的分类提供一个指导。

公共网络和专用网络是两种广泛的网络类别。公共网络，通常指任何人都可接入的网络，互联网是一个最常见的例子，由于这些数据交换设施都是公共的，故而其信任级别是相对较低的，风险则较高，因此这需要更多的措施来降低一些有可能的风险，比如安全网关等。专用网络，一般指由本机构拥有或租用线路构成的网络，也可以称为私有网络，对于需要传输资产价值较高的数据，比如包含健康数据在内的个人敏感数据时，比起接入公共网络，接入专用网络通常风险更低。

一般情况下网络连接架设可以在组织内部，不同组织之间，亦或是组织与公共区域之间。公共网络通常情况下是不同组织之间或者组织与公共区域之间。专用网络通常是架设在组织内部或者不同组织之间，但对于一些远程用户，也可以使用虚拟专用网络(VPN)，这相当于在组织与公共区域(公用网络)上建立专用网络，进行加密通信。

个域网(Personal Area Network，PAN)、局域网(Local Area Network，LAN)和广域网(Wide Area Network，WAN)为产品网络预期接入的不同的域。通常情况下，局域网是一个组织内部的本地节点之间互联形成的域，通常这种网络是相对封闭的。而广域网一般情况下是使用电信供应商提供的网络设施将多个局域网或节点组成的范围更广的域，当然这也会引入更多的网络安全方面的风险。而个域网在某些认知中被认为是局域网的一种，但网络互连技术发展至今日，个域网的应用也越发广泛，尤其是无线个域网(WPAN)，其包括了蓝牙、HomeRF 等通信技术，而接入个域网时，这些技术所带来的风险也需要制造商去考虑。

对于使用场景，总的来说分为医疗场景和非医疗场景，但是建议制造商在陈述使用场景进行分类时，仍需要进一步的分析不同使用场景中不同的用途(见 4.1.2.5 注释)，在不同的用途下，其可能遭受的网络安全风险的程度也是不同的。

因此，不同分类的组合所可能遭遇的风险也是不一样的，在这个分类的样例(表 C.1)中使用了一个监护类产品作为例子。

表 C.1　分类的样例

使用场景	域类型	网络类型	连接类型	数据传输方向
监护场景	局域网	专用网络	有线网线	双向传输
监护场景	局域网	专用网络	无线 wifi	双向传输
远程维护场景	广域网	公共网络	有线网线	单向向内传输
本地维护场景	—	—	有线 USB	单向向内传输
数据导出	—	—	有线 USB	单向向外传输

条款 4.1.3.4　列明所有第三方和包含在产品中的开源软件的目标主要是让测试者更清楚地了解产品的情况。多数的情况下，获知那些广为人知的第三方软件或开源软件可以帮助测试者初步的判断其网络安全的风险，这样的活动有利于接下来对产品的网络安全能力进行测试。

条款 4.1.7　用户访问控制的细节可能包括密码的强度、不成功尝试的次数限制、禁止访问的条件和后果、反自动破解的保护功能、密码要求被更新的频次等。

制造商需要考虑为了提权或越过用户访问控制措施的攻击带来的风险，而且若设计了这样的风险控制措施则需要在网络安全能力说明中陈述。但显而易见的是，这样的攻击的方式是未知的，且是具有发展性的，因此并不是说实现了某些风险控制措施防止攻击便可以称其为“本产品可以抵御所有攻击”。

另外，用户访问控制需要考量与可得性之间的关系，有些用户访问控制措施，例如，多次尝试不正确的访问会引起一段时间之内拒绝访问，这有可能导致可得性变差，甚至会间接导致一些不可接受的安全性方面的风险。因此制造商需要考虑这种情况以避免单方面为了提升访问控制而将可得性降低到不可接受的水平。

条款 4.1.11　考虑到某些产品在特定的情况下，在 HDO 的部署责任方是制造商，那么在这种情况下，制造商要对传输过程中敏感数据的完整性负责。因为对于一些产品，在传输某些指令时，指令失去完整性会影响安全性。可能更多场合，传输完整性的责任是 HDO，但公钥、秘钥的管理、数据加密解密需要由 HDO 和制造商共同实现，但往往这种情况下，并不是产品本身的网络安全能力，因此并不在本文件的范围内。

条款 4.1.14　系统固化被认为是在应用软件难以修改或者不方便修改的前提下提高整体安全性的最有效的手段。合理的系统固化能够消除系统上存在的已知漏洞，减小攻击接口，提升产品整体安全等级。

是否需要实施固化是需要制造商通过风险分析来确认的，当然这也关乎于实施固化的责任方，下面则提供了几个实施固化责任方的举例。

——若产品是 ME 设备或 ME 系统，且至少包含一套操作系统，则对操作系统的固化的责任方一般为制造商。

——若产品是 ME 设备或 ME 系统，制造商承担了部署软件的责任，且会提供部署软件的平台/操作系统，那么制造商亦是操作系统的责任方。

——若产品为/包含软件，但预期产品会安装在 HDO 提供的平台/操作系统上，则操作系统的责任方可能不为制造商。但这并不意味着制造商不需要去考虑不实施固化所带来的的风险。

条款 4.1.16　抗抵赖性即是不可否认性，也就是说节点 A 到节点 B 的传输完成后，节点 A 不能否认是节点 A 传给节点 B 的。抗抵赖性具有双向性，一方面是数据发送方不可抵赖其发送数据的行为，一方是数据接收方不可抵赖其接收数据的行为。这可以通过数字签名和时间戳等手段来保证，这样的方式同时可以保证对象和资源的真实性。

抗抵赖性的实现原理可以是基于数字签名技术，我们知道基于签名及签名验证，可以判断数据的发送方是真实存在的用户。同时，通过对签名的验证，可以判断数据在传输过程中是否被更改。从而，可

以实现数据的发送方不能对发送的数据进行抵赖，发送的数据是完整的，实现产品的抗抵赖性和完整性需求。如果有需要，对于B/S架构和C/S架构，都需要采用基于签名及签名验证的实现原理。对于B/S架构，客户端数据签名模块以控件的方式，配置在需要进行签名的网页中，供用户访问时下载。对于C/S架构，客户端数据签名模块以动态库的方式，供专业客户端软件调用。

当然，抗抵赖性也可通过用户访问控制、节点认证、健康数据的数字签名、时间戳等方式联合实现，虽然上述了一些技术上的举例，但本文件并不限制实现抗抵赖性的手段。

条款4.1.17 目标是为了确保健康数据未经非授权改动或销毁，并且来自发起人，即是“确保用户所见即为真”。数字签名是一种典型的保证健康数据来自发起人手段。当然这也需要在节点认证的时候，需要保证节点的真实性。而保证完整性，则需要使用其他的手段。

条款4.1.18 允许机构的安全官员对活动进行审计，评估对安全域策略的遵守情况，检测违规行为的实例，并便于发现不正确的创建、访问、修改和删除受保护的个人敏感数据。对于审计日志，产品应能够维护所有与安全相关的事件的一个或多个日志。

条款4.1.19 保存、以临时文件形式存储和长期存储是有区别的，否则对临时存储健康数据的设备去要求需要数据备份可能是不公平的(例如，床旁监护仪、注射泵等)，这样会增加此类设备的不必要的成本，是否需要提供数据备份与灾难恢复的手段应通过制造商对产品的风险分析来确定。

制造商需要基于风险分析，考虑是否制定灾难恢复计划/策略，以对产品的关键数据进行恢复，达到满足最低临床需求。当然，这样的策略应是灵活的，用以应对不同HDO的不同实际需求，可能需要释放一些相关的配置权限给HDO IT。这意味着产品需要支持备份和恢复产品的配置和自定义设置(包括安全设置和账号信息)。

另外，有些为了增加产品可用性(usability)，让产品意外中断之后能够恢复到上一次的工作流程而进行的实时保存和恢复并不是本条的目标。

条款4.1.20.2 目标是敦促制造商对第三方操作系统等第三方组件在产品生命周期过程中所带来的网络安全风险的关注。

条款4.1.20.3 目标是希望产品中第三方安全补丁是最新的，进而保证产品不存在已知的高风险漏洞，但有可能只会在测试时来确认这些补丁(包括病毒库)是否为最新。日常的监管中则可能是一种定期的行为，而对这样的行为的规范并不在本文件中规定。

如果供应商/制造商提供了产品的维护，且明确要求产品应不定期进行恶意软件的探测，则安全软件(包括病毒库、木马库等)应被更新，操作系统和应用程序被及时打上补丁。

条款4.3.3 本文件并没有对口令的复杂度做出要求。因为在某些临床应用当中，复杂的口令可能会限制产品的易用性/可用性，因此对于这些临床应用，简单的密码可能是必不可少的，但这需要制造商提供一定的说明来解释使用简单密码的原因，并且必要时要通过风险分析的方式来证明简单密码不会造成其他危害。

同一类或不同型号的同类产品不宜保持同样的默认凭证，以防止知道其中一台产品的默认凭证就知道了全部产品的默认凭证。

条款4.3.5 在大多数场景下，最终用户(操作者)可能会离开设备一段时间，在这段时间内，可能会发生未授权的用户对程序或系统进行访问而不需要身份验证的情况，这样的情况在一些临床应用的场景下是危险的，尤其是那些辐射剂量较大的诊断场景。此外，这段时间也有可能未授权的用户窃取或破坏健康数据。因此，管理员在设置时间时，应考虑这些临床应用场景。但在另外一些临床应用中，操作者对应用程序的需求可能只是查看应用程序提供的影像数据而并非经常会去操作应用程序，类似于这样的场景下，则可能需要关闭自动锁定或注销的功能，否则可能会严重影响产品的可得性，当然，在这种情况下，网络安全风险也应是可接受的。

条款4.3.6 在紧急情况下，临床用户需要能够访问健康数据，而无需个人用户标识和身份验证[中断功能(breaking-glass)]。紧急访问将被检测、记录和报告，这意味着紧急访问至少能够被审计记录。理想

情况下，包括某种方式立即通知系统管理员或医务人员（除审计记录外）。紧急访问的功能可能有各种不同的产品设计对应的产品实现，这可能是无需验证或者是简单的验证，HDO 可通过使用特定用户账户或系统功能的程序方法解决此问题。管理员需要能够启用/禁用依赖于技术或程序控制的产品提供的任何应急功能。

附 录 D
（资料性）
本文件关于个人敏感数据的考量

D.1 应明确本产品是否具备持有、显示、传输个人敏感数据的能力。

D.2 应明确本产品是否持有如下种类的个人敏感数据：

——应明确人口统计学信息（如：姓名、联系地址、定位地址、证件号码）；

——应明确病史信息（如：病史编号、账号、检查或治疗的日期、所使用医疗器械编号）；

——应明确诊断与治疗信息（如：摄影/透视、检查结果、可供推断身份的生理数据）；

——应明确由设备使用者或操作者自由输入的文本信息；

——应明确生物认证数据（如：指纹、虹膜、面容）；

——应明确个人财务信息（如：信用卡号、健康保险信息）。

注：比如某位医生在自由输入的字段里包含了病人的姓名。这是可能存在漏洞的地方，需要披露。

D.3 应明确本产品对个人敏感数据的持有方式，这可能包括：

——暂存于挥发性存储器中（断电或复位后被清除）；

——永久保持在本地存储介质中；

——导入/导出；

——在重大维护间期内继续持有个人敏感数据。

注：如医疗器械在维护期间内部保存有个人敏感数据，则可能需要跟设备维护商签订保密协议。

D.4 个人敏感数据的传输、导入/导出机制，这可能包括：

——个人敏感数据的显示；

——生成包含个人敏感数据的硬拷贝报告或镜像文件；

——基于移动存储介质的个人敏感数据导入/导出（如：移动盘、光盘、磁带、存储卡等）；

——基于特定电缆的个人敏感数据交换（如：IEEE 1073、串行端口、USB、FireWire 等）；

——基于有线网络连接的个人敏感数据交换（如：LAN、WAN、VPN、局域网、英特网等）；

——基于无线网络连接的个人敏感数据交换（如：WiFi、蓝牙、红外线等）；

——通过扫描方式导入个人敏感数据；

——其他。

参 考 文 献

[1] 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

[2] 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

[3] 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

[4] 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

[5] GB/T 25068.1—2020 信息技术 安全技术 网络安全 第1部分:综述和概念

[6] GB/T 29246—2017 信息技术 安全技术 信息安全管理体系 概述和词汇

[7] GB/T 35273—2020 信息安全技术 个人信息安全规范

[8] GB/T 37964—2019 信息安全技术 个人信息去标识化指南

[9] YY/T 0287—2017 医疗器械 质量管理体系 用于法规的要求

[10] YY/T 0316—2016 医疗器械 风险管理对医疗器械的应用

[11] 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

[12] T/ZMDS 20001—2016 风险管理在IT网络引入医疗器械时的应用 第1部分:角色、责任与活动

[13] 医疗器械网络安全注册技术审查指导原则(国家食品药品监督管理总局通告2017年第13号)

[14] 医疗器械网络安全技术审查指导原则(第二版)(征求意见稿)

[15] 医疗器械软件注册技术审查指导原则(国家食品药品监督管理总局通告2015年第50号)

[16] 医疗器械软件技术审查指导原则(第二版)(征求意见稿)

[17] ISO/IEC 27033-1:2015 Information technology—Security techniques—Network security—Part 1:Overview and concepts

[18] ISO/IEC 29167-19:2016 Information technology—Automatic identification and data capture techniques—Part 19:Crypto suite RAMON security services for air interface communications

[19] ISO/IEC 80001-5-1 Application of Risk Management for IT networks incorporating medical device—Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software—Part 5-1: Activities in the product life-cycle

[20] ISO/TR 80001-2-6:2014 Application of risk management for IT-networks incorporating medical devices—Part 2-6: Application guidance—Guidance for responsibility agreements

[21] ISO/TR 80001-2-7:2015 Application of risk management for IT-networks incorporating medical device—Application guidance—Part 2-7: Guidance for Healthcare Delivery Organizations (HDOs) on how to self-assess their conformance with IEC 80001-1

[22] IEC 80001-1: 2010 Application of risk management for IT-networks incorporating medical devices—Part 1: Roles, responsibilities and activities

[23] IEC/TR 60601-4-5 Medical electrical equipment—Part 4-5: Safety related technical security specifications for medical devices

[24] IEC/TR 80001-2-1:2012 Application of risk management for IT-networks incorporating medical devices—Part 2-1: Step-by-step risk management of medical IT-networks—Practical applications and examples

[25] 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

[26] IEC/TR 80001-2-3:2012 Application of risk management for IT-networks incorporating medical devices—Part 2-3: Guidance for wireless networks

[27] IEC/TR 80001-2-4:2012 Application of risk management for IT-networks incorporating medical devices—Part 2-4: Application guidance—General implementation guidance for healthcare delivery organizations

[28] IEC/TR 80001-2-5:2014 Application of risk management for IT-networks incorporating medical devices—Part 2-5: Application guidance—Guidance on distributed alarm systems

[29] IEC/TR 80001-2-8:2016 Application of risk management for IT-networks incorporating medical devices—Part 2-8: Application guidance—Guidance on standards for establishing the security capabilities identified in IEC/TR 80001-2-2

[30] IEC/TR 80001-2-9 Application of risk management for IT-networks incorporating medical devices—Part 2-9: Application guidance—Guidance for use of security assurance cases to demonstrate confidence in IEC/TR 80001-2-2 security capabilities

[31] AAMI TIR57:2016 Principles for medical device security—Risk management

[32] ANSI/NEMA HN 1—2019 American National Standard— Manufacturer Disclosure Statement for Medical Device Security

[33] UL 2900-1: 2017 Standard for Software Cybersecurity Network-Connectable Products, Part 1: General Requirements

[34] UL 2900-2-1 STANDARD FOR SAFETY Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems

[35] IMDRF/CYBER WG/N60 FINAL:2020, Principles and Practices for Medical Device Cybersecurity, 2020.4.

[36] FDA, Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, 2014.10.

[37] FDA, Content of Premarket Submissions for Management of Cybersecurity in Medical Devices Draft, 2018.10.

[38] FDA, Postmarket Management of Cybersecurity in Medical Devices, 2016.12.

[39] MDCG 2019-16 Guidance on Cybersecurity for medical devices