ICS 35.240.80

ZMDS

中关村医疗器械产业技术创新联盟团体标准

T/ZMDS 20003-2019

医疗器械网络安全风险控制 医疗器械网络安全能力信息

Medical device security risk control
– information of medical device security capabilities

2019-11-18 发布　　2019-11-18 实施

中关村医疗器械产业技术创新联盟　　发布

目　次

前　　言

原国家食品药品监管总局于 2017 年 1 月 20 日发布的《医疗器械网络安全注册技术审查指导原则》对医疗器械制造商在保障网络安全方面提供了重要的指导。有企业在使用该指导原则时，对指导原则中所提到的网络安全能力希望得到进一步的解释。从医疗器械制造商的角度出发，需要有一份标准来使网络安全能力得到解读，以便于更好地实现对医疗器械网络安全的风险控制。

本标准按照 GB/T 1.1-2009 给出的规则起草。

本标准由中关村医疗器械产业技术创新联盟提出。

本标准由中关村医疗器械产业技术创新联盟标准化技术委员会归口。

本标准起草单位有：飞利浦（中国）投资有限公司、北京怡和嘉业医疗科技股份有限公司、北京市医疗器械技术审评中心、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、北京谊安医疗系统股份有限公司、北京品驰医疗设备有限公司、通用电气医疗集团、上海西门子医疗器械有限公司、上海联影医疗科技有限公司、西门子(深圳)磁共振有限公司。

本标准主要起草人：谌达宇、陈蓓、陈然、巩玉香、殷骏、刘建勋、王威、陈浩、孙卓惠、秦川、朱雷、陈恒、杨柳恩、侯丙营、李俊霖、丛玉孟、曹青。

引　　言

医疗器械在运行过程中，会产生并处理大量的数据。这些数据可以用于疾病的诊断、治疗与预防，也可以用于科学研究、流行病分析与预测，同样也可以用于商业趋势分析、目标群体预测、广告精准投放。然而，在不法之徒手里，它们会被用于获取隐私、骗取信任、贩卖信息、绑架数据，甚至会被用于造成直接的人身伤害。由于医疗健康数据属于重要的隐私数据，同时又具有较高的价值，保护医疗器械的网络安全也就成为一件不可或缺的工作。从现实的角度而言，以医疗系统为攻击目标的网络安全事件屡有发生，信息窃取，数据绑架时有耳闻。《中华人民共和国网络安全法》于 2017 年 6 月 1 日开始实施，医疗器械的网络安全是社会整体网络安全中的一个重要组成部分，现实状况也亟需我们认真地对待医疗器械的网络安全问题。

通常，医疗器械网络的拥有者是医疗服务提供方，从资产角度而言，网络的建立、部署、配置、调整、维护、运营、停用均由医疗服务提供方来控制，医疗器械的联网策略服从于医疗服务提供方的网络政策；从数据的角度而言，医疗服务提供方常常担任数据控制者的角色；医疗器械制造商虽然参与了数据处理，但在权责分配上其角色并不属于数据控制者。网络与数据两方面的原因都使得医疗服务提供方成为网络安全的责任方。医疗器械制造商与信息设施提供方需要配合责任方，共同实现对医疗器械网络安全的保障。简言之，医疗器械的网络安全是由责任方（医疗服务提供方）、信息设施提供方、医疗器械制造商三者共同参与而予以保证的。抛开三者中的任何一方、或者单独只考虑三者中的任意一方来谈网络安全，都是不明智的，这不仅仅使得网络安全很难得到保障，还会导致整个网络安全保障的经济成本提高。

医疗器械制造商在实践过程中成功地使用了风险管理体系来进行医疗器械的安全性与有效性的管理。由于医疗器械网络安全的破坏一方面可能导致传统的安全有效性受损，另一方面，数据破坏也同样属于资产的损失。于是当处理医疗器械的网络安全问题时，自然地也将网络安全纳入其风险管理的范畴。

由 YY/T 0316-2016 的 6.2 条规定，降低风险的控制措施存在三个不同的优先层级，分别是固有安全措施、保护性安全措施和信息性安全措施。其中固有安全措施为首选措施，而信息性安全措施是作为最末选项而出现的。然而，由于实现条件、实施成本、责权归属、专业领域等诸多实际情况的约束，很多风险控制措施不得不通过信息性安全措施来实现。而且部分网络安全风险控制措施必须要责任方与信息设施提供方、医疗器械制造商实现三方联动才能实施，信息性安全措施虽然优先级最低，但仍然是十分重要的。由于医疗器械制造商的专业领域、权责范围所限，部分网络安全的风险控制措施交由专业的网络安全人员或组织来实施不仅仅会很大程度地降低成本，而且往往能实现更佳的网络安全保障。信息性安全措施要求医疗器械制造商与责任方进行充分的信息披露，以实现网络安全保护的最大社会经济效益。这也是 IEC 80001 系列标准十分重视医疗器械制造商与责任方之间信息沟通的原因。医疗器械制造商需要根据医疗器械的预期用途、使用场景、核心功能来选取合适的风险控制措施。信息性安全措施是网络安全保障中不可或缺的组成部分。

IEC 80001 系列标准所总结的 19 项网络安全能力规范了医疗器械制造商与责任方之间的沟通范围与内容，也成为医疗器械制造商考虑网络安全控制措施时的一个重要的参考。HIMSS NEMA HN 1-2013 标准进一步地对这些网络安全能力进行了一个问卷式的分解，使得网络安全能力不再是抽象的概念，而是便于理解、便于实施的具体清单。对医疗器械制造商与责任方之间的信息沟通提供了很大的帮助。属于信息性风险控

制的一个重要组成部分。

由于这些标准中所提及的 19 项网络安全能力被业界所广泛接受，其本身构成了一个快速了解网络安全问题的清单，医疗器械监管部门对此也表示了认可。《医疗器械网络安全注册技术审查指导原则》将此 19 项网络安全能力列入了网络安全技术考量的范畴。由于指导原则本身没有义务对这些网络安全能力进行定义与解释，也就需要从标准的角度比较明确地提供一个参考。这也就是本标准得以起草的一个直接成因。

本标准的编制是由中关村医疗器械产业技术创新联盟、北京市医疗器械技术审评中心及部分医疗器械制造商的合作下完成的，旨在对医疗器械网络安全相关的信息披露提供指导。

医疗器械网络安全风险控制　医疗器械网络安全能力信息

1　范围

本标准适用于以下医疗器械产品：

1）具有网络连接功能以进行电子数据交换或远程控制的医疗器械产品；

2）采用存储媒介以进行电子数据交换的医疗器械产品。

本标准适用于以下两类角色：

1）医疗服务提供方

医疗服务提供方对提供有效的网络安全管理负有最终责任。医疗服务提供方应采用行政、物理和技术等相关维度的管理措施来有效保护医疗信息安全并遵守相关法律法规的规定。医疗服务提供方可以向医疗器械制造商索取本标准所述的网络安全能力相关的信息，并参考此信息来执行网络安全风险管理。

2）医疗器械制造商

医疗器械制造商对医疗器械网络安全能力的影响是在医疗器械中加入网络安全功能或措施，以协助医疗服务提供方进行有效的网络安全风险管理。制造商应充分评估来自医疗服务提供方的需求、医疗器械的预期用途、使用场景与核心功能，在医疗器械产品的研发、生产、安装、维护过程中考虑本标准所描述的网络安全能力相关要求。

2　术语与定义

2.1　自动注销 AUTOMATIC LOGOFF (ALOF)

设备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。比如, 用户可以设定系统的闲置超时时间，超时后进行自动锁定，保障健康数据在系统无人值守时不受破坏。

2.2　审核控制 AUDIT CONTROLS (AUDT)

为可靠审核数据被何人以何种方式予以处理而规定的协调统一的方法，以便于医疗服务提供方的信息部门能够利用共有的机制、标准和技术来进行监视。 通过审核踪迹对系统和数据的访问、修改或删除予以记录，从而跟踪和检查系统的活动。

2.3　授权 AUTHORIZATION (AUTH)

防止未经授权而访问系统的数据和功能，保持数据的保密性、完整性和可得性以及防止系统功能对非授权用户的开放。根据医疗服务提供方 IT 政策的规定，用户的身份在经验证后，应只能访问其获准访问的

数据，且只能使用其获准使用的设备功能。

2.4 安全特性配置（CONFIGURATION OF SECURITY FEATURES - CNFS）

该功能使得经授权的 IT 管理员能够配置产品的网络安全能力，来满足医疗服务提供方的策略和工作流程。

2.5 网络安全产品升级（CYBER SECURITY PRODUCT UPGRADES – CSUP）

以一致的方式，由经授权的现场服务人员、远程服务人员，或由经授权的医疗服务提供方人员来对产品网络安全补丁进行安装或升级。

2.6 健康数据身份信息去除（HEALTH DATA DE-IDENTIFICATION – DIDT）

设备（含应用软件或者附加工具）能够直接删除或隔离*可识别出患者身份的信息。

注：例如体系结构设计使得远程维护人员无法取得设备上的患者身份信息。

2.7 数据备份与灾难恢复（DATA BACKUP AND DISASTER RECOVERY – DTBK）

确保医疗服务机构在数据、硬件或者软件遭到损坏或者损毁后可以继续开展业务。

注：本项要求不适宜于某些小型、低成本的医疗器械；也不适宜于某些具有能力采集新一轮数据的医疗器械（如：无线网络的短暂断开导致心率数据的短暂丢失）

2.8 紧急访问（EMERGENCY ACCESS – EMRG）

在急救场景下，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访问健康数据。 紧急访问机制仍然可能要求用户登记经自我声明（未经认证）的用户身份，紧急访问的相关信息会被系统检测、记录和报告。

2.9 健康数据完整性与真实性(HEALTH DATA INTEGRITY AND AUTHENTICITY – IGAU)

保证健康数据的来源正确，且不会在未经授权的情况下被更改或者毁坏，确保健康数据的真实性。

2.10 恶意软件探测与防护（MALWARE DETECTION/PROTECTION – MLDP）

产品满足监管、医疗服务提供方和使用者的要求，有效地防护、探测和去除恶意软件的能力。由于恶意软件会不断更新，因此操作系统和应用程序要及时打补丁。

2.11 网络节点鉴别（NODE AUTHENTICATION – NAUT）

提供或支持某种节点身份验证措施，以确保数据的发送方与接收方互相识别并被授权进行数据传输。

2.12 人员鉴别（PERSON AUTHENTICATION – PAUT）

为用户创建独有的帐号，并为连接网络的设备创建基于角色的访问控制机制来对人员身份进行认证。对设备、网络资源以及健康数据的访问权限进行控制，并生成不可否认的审核踪迹。

2.13 物理锁（PHYSICAL LOCKS ON DEVICE – PLOK）

用物理的方式确保非授权的访问无法损害系统或数据的保密性、完整性和可得性。合理地保证存储在产品或者媒介上的健康数据持续安全，且安全程度与设备上所存储的数据的敏感性和容量相适应。

2.14 第三方组件维护计划（THIRD-PARTY COMPONENTS IN PRODUCT LIFECYCLE ROADMAPS – RDMP）

为使产品在其完整生命周期中能满足相关的内部质量体系和外部法规的要求，在产品完整生命周期中，制造商对各个组件生命周期的影响进行前瞻性的管理。产品所涉及的第三方软件包括操作系统、数据库系统、报告生成器等。

2.15 系统与应用软件硬化（SYSTEM AND APPLICATION HARDENING – SAHD）

在保持产品预期用途不变的条件下，调整医疗器械和应用软件方面的安全控制措施，实现信息安全最大化（硬化），如：通过关闭端口、移除服务等，将涉及产品的攻击矢量与整体攻击面最小化。

2.16 安全指导（SECURITY GUIDES – SGUD）

为系统的操作者和管理员提供安全指南。

2.17 健康数据存储保密性（HEALTH DATA STORAGE CONFIDENTIALITY – STCF）

医疗器械制造商建立技术控制措施，以降低存储在产品或者可移动媒介上的健康数据的完整性和保密性受到潜在威胁的可能性。

2.18 传输保密性（TRANSMISSION CONFIDENTIALITY – TXCF）

为满足相关法规和标准的要求，制造商应采取措施，使得在经认证的节点间传送健康数据时，保持数据的保密性，以便于在相对开放的网络和/或在相对严苛的保密环境中进行健康数据的可靠传输。

2.19 传输完整性（TRANSMISSION INTEGRITY – TXIG）

设备保证传输过程中能够维系健康数据的完整性， 以便于在相对开放的网络和/或在相对严苛的保密环境中进行健康数据的传输。

2.20 责任方 RESPONSIBLE ORGANIZATION

对医疗器械网络的使用与维护承担责任的实体。

示例：如：医院、私人医生或医疗机构。

注：根据 IEC 60601-1:2012 第 3.101 条修改。

2.21 **关键特性** KEY PROPERTIES

被置于风险管理中的三个医疗 IT 网络特性（安全性、有效性、数据与系统信息安全）。

3 医疗器械制造商信息披露要求

3.1 总则

制造商应按本标准要求披露网络安全能力信息，配合责任方进行其医疗 IT 网络风险管理。

3.2 产品描述信息

制造商应向责任方披露如下信息：

– 产品类别
  根据《医疗器械分类目录》判定的产品类别，可用数字表示

– 产品名称与型号

– 制造商联系信息
  提供网络安全信息披露相关负责人或部门的联系方式

– 预期连网用途
  提供连网的目的，简要描述连网所实现的功能

3.3 隐私数据管理

制造商应向责任方披露如下信息：

a) 本医疗器械对是否具备持有、显示、传输隐私数据的能力？

b) 本医疗器械是否持有如下种类的隐私信息：

  b.1 人口统计学信息（如：姓名、联系地址、定位地址、证件号码）

  b.2 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）

  b.3 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）

  b.4 由设备使用者或操作者自由输入的文本信息*

  b.5 生物认证数据（如：指纹、虹膜、面容）

  b.6 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。

c) 本医疗器械对隐私数据的持有方式：

c.1 本医疗器械是否将隐私数据暂存于挥发性存储器中？（断电或复位后被清除）

c.2 本医疗器械是否将隐私数据永久保持在本地存储介质中？

c.3 本医疗器械是否支持将隐私数据导入/导出到其它系统？

c.4 本医疗器械是否在重大维护间期内继续持有隐私数据？*

注*：如医疗器械在维护期间内部保存有隐私数据，则可能需要跟设备维护商签订保密协议。

d) 隐私数据的传输、导入/导出机制。

d.1 本医疗器械是否能显示隐私数据？

d.2 本医疗器械能否生成包含隐私数据的硬拷贝报告或镜像文件？

d.3 本医疗器械是否支持基于移动存储介质的隐私数据导入/导出？（如：移动盘，光盘，磁带，存储卡等）

d.4 本医疗器械是否支持基于特定电缆的隐私数据交换？（如：IEEE 1073，串行端口，USB，FireWire等）

d.5 本医疗器械是否支持基于有线网络连接的隐私数据交换？（如：LAN，WAN，VPN，局域网，英特网等）

d.6 本医疗器械是否支持基于无线网络连接的隐私数据交换？（如：WiFi，蓝牙，红外线等）

d.7 本医疗器械是否支持通过扫描方式导入隐私数据？

d.8 是否存在其它的隐私数据传输、导入/导出机制？

3.4 网络安全能力披露

3.4.1 自动注销能力 ALOF

制造商应回答下述问题，向责任方披露医疗器械的本项网络安全能力：

a) 当预设时间段内医疗器械无人操作时，能否配置医疗器械，使其自动登出，若需继续使用，则要求用户再次输入身份确认信息？（如：自动登出，会话锁定，带口令屏保）

a1) 无人操作的预设时间段能否由用户或管理员进行配置？

a2) 系统自动锁定后，能否由用户手工解锁？

3.4.2 审核控制能力 AUDT

制造商应回答下述问题，向责任方披露医疗器械的本项网络安全能力：

a) 本医疗器械是否具有保留审核踪迹的能力？

b) 如保留审核踪迹，如下事件是否被记录？

– 登入、登出

– 隐私数据被显示，打印或以其它方式呈现

– 数据的增、改、删

– 基于移动存储介质的导入、导出数据

– 基于外部连接（如网络连接）的导入、导出数据

– 医疗器械的远程维护

– 上述事件之外的其它事件记录，如有，应说明。

c) 在审核踪迹事件记录中，每个事件相关的如下识别信息是否被保留？

– 用户身份标识

– 日期、时间。如有，说明系统时间是否有网络同步。

3.4.3 确定用户授权的能力 AUTH

制造商应回答下述问题，向责任方披露医疗器械的本项网络安全能力：

a) 医疗器械是否具有用户登录或其它措施，防止未经授权的用户进入？如有，应说明采用了何种技术措施（如：口令、生物认证、钥匙卡等）

b) 医疗器械能否区分用户身份而给予不同的权限？（如：访客、日常用户、高级用户、管理员等）

c) 医疗器械的拥有者、操作者能否获得不受限制的权限？（如：通过管理员账号、或通过获取根权限的方式进入操作系统或应用程序）。若医疗器械支持多个高权限账号（如：管理员，根账号），制造商应加注说明。若制造商对管理员账号的使用施加限制，可以加注予以说明。

3.4.4 安全特性配置能力 CNFS

制造商应回答下述问题，向责任方披露医疗器械的本项网络安全能力：

a) 医疗器械的拥有者、操作者是否能重新配置产品的网络安全能力？如制造商对用户重新配置医疗器械的网络安全能力予以限制，则应加注说明。

3.4.5 网络安全升级能力 CSUP

制造商应回答下述问题，向责任方披露医疗器械的本项网络安全能力：

a) 当相关操作系统或医疗器械发布了网络安全补丁时，是否许可用户自行安装相应补丁？若制造商限制用户自行安装操作系统或医疗器械的网络安全补丁，则应对此类限制加注说明。

a1) 网络安全补丁或其它软件能否被远程安装？若制造商限制用户远程安装操作系统或医疗器械的网络安全补丁，则应对此类限制加注说明。

3.4.6 健康数据身份信息去除能力 DIDT

制造商应回答下述问题，向责任方披露医疗器械的本项网络安全能力：

a) 医疗器械是否内置了隐私数据的去标识化能力？如适用，制造商应加注说明所用的匿名化标准或指导原则。若此能力可被配置，也应加注说明。

注：可参考国家标准 GB/T 37964-2019《信息安全技术个人信息去标识化指南》

3.4.7 数据备份与灾难恢复能力 DTBK

制造商应回答下述问题，向责任方披露医疗器械的本项网络安全能力：

a) 医疗器械是否存在内置的数据备份能力？（如：备份到远程存储设备或备份到磁带、盘片等移动存储介质）

3.4.8 紧急访问隐私数据的能力 EMRG

制造商应回答下述问题，向责任方披露医疗器械的本项网络安全能力：

a) 医疗器械是否具备紧急受访的特性？

3.4.9 数据完整性真实性确认能力 IGAU

制造商应回答下述问题，向责任方披露医疗器械的本项网络安全能力：

a) 医疗器械是否通过隐式或显式的错误探测、错误纠正，对存储数据的完整性予以保障？

注：本问题仅针对存储数据的完整性。

3.4.10 恶意软件的探测与防护能力 MLDP

制造商应回答下述问题，向责任方披露医疗器械的本项网络安全能力：

a) 医疗器械是否支持反恶意软件（或其它反恶意软件机制）？

a1) 可否由用户自己配置或重新配置反恶意软件？

a2) 探测到恶意软件时，是否通过用户界面予以通知？

a3) 探测到恶意软件时，是否仅能由经制造商授权的人员对系统进行修复？

b) 能否由医疗器械拥有者安装或升级反病毒软件？

c) 由制造商安装的反病毒软件，其病毒特征库的升级能否由医疗器械的拥有者、操作者来完成？

3.4.11 网络节点鉴别能力 NAUT

制造商应回答下述问题，向责任方披露医疗器械的本项网络安全能力：

a) 医疗器械是否提供或支持某种节点身份验证措施，以确保数据的发送方与接收方互相识别并被授权进行数据传输？

3.4.12 人员鉴别能力 PAUT

制造商应回答下述问题，向责任方披露医疗器械的本项网络安全能力：

a) 医疗器械是否对至少一个用户提供用户名/口令的识别方式？若不是采用用户名/口令的识别方式，可加注说明。

a1) 医疗器械是否支持多个用户使用各自不同的用户名与密码？

b) 医疗器械能否配置为接受外部认证服务器对用户的授权？（如：微软的 Active Directory，NDS(Netware Directory Services)，LDAP 等）如能，则加注说明属于何种机制。

c) 医疗器械能否配置为某个用户多次登录失败后，禁止其继续尝试？如能，则加注说明具体做法。

d) 初始密码能否在安装时刻，或在在安装前予以修改？制造商如施加特定的限制，则应加注说明。

e) 除去紧急账号，系统是否有意设计为存在着多个用户共享的账号？如存在这样的设计，则加注说明其用途是为了医疗器械维护还是为了医疗器械使用，并说明账号与口令是否在多个同型号医疗器械上都相同。

f) 医疗器械是否能让责任方对账号口令复杂度进行配置？如制造商对口令的复杂度有限制，则加注说明。

g) 账号口令是否可配置为定期失效？如是，加注说明失效周期或管理方法。

3.4.13 物理锁保护能力 PLOK

制造商应回答下述问题，向责任方披露医疗器械的本项网络安全能力：

a) 除去移动介质外，医疗器械是否对包含隐私数据的部件提供物理保护？（如：必须使用工具、钥匙才能取出存储部件）

3.4.14 第三方组件维护能力 RDMP

制造商应回答下述问题或给出描述，向责任方披露医疗器械的本项网络安全能力：

a) 列出所提供的或所需的（需额外购买的或随产品附带的）操作系统，并注释版本号。

b) 制造商所提供的第三方软件是否有清单列示？如有，列出相应清单。如存在专属组件，则应注明相应信息能否在售前索取到。

3.4.15 系统与应用加固能力 SAHD

制造商应回答下述问题，向责任方披露医疗器械的本项网络安全能力：

a) 制造商对医疗器械是否采取了网络安全加固措施？

b) 医疗器械是否具有某种机制来判断所安装的程序、升级包是经过制造商授权的？（如：哈希值、校验码等）

c) 医疗器械是否具有外部通信能力？（如：网络、调制解调器、等）如有，则注释说明外部通信是否必须要由本医疗器械发起，或本医疗器械只是接受通信请求。

d) 文件系统是否许可文件层次的访问控制（如：Windows 平台的 NTFS）？如许可，简要注释说明文件层次访问控制的情况，如文件层次的访问权限属于普通用户权限还是管理员权限，是否许可远程访问还是必须本地访问，等。

e) 与预期用途无关的用户账号，应用软件账号是否已经全部删除或关闭？注释说明在安装前、安装过程中需要删除、关闭的账号，或者需要最终用户来关闭的账号。

f) 与预期用途无关的共享资源（如：共享文件）是否被全部禁用？注释说明在安装前、安装过程中需要关闭的，或者需要最终用户来禁用的共享资源。

g) 与预期用途无关的通信端口是否被全部关闭、禁用？注释说明在安装前、安装过程中需要关闭、禁用的，或者需要最终用户来关闭、禁用的端口。

h) 与预期用途无关的服务（如：telnet、FTP、IIS 等）是否被全部关闭、禁用？注释说明在安装前、安装过程中需要关闭、禁用的，或者需要最终用户来关闭、禁用的服务。

i) 与预期用途无关的应用软件（商品现货软件或者如 IE 浏览器一类由操作系统自带的软件）是否被全部删除、禁用？注释说明在安装前、安装过程中需要删除、禁用的，或者需要最终用户来禁用的应用软件。

j) 医疗器械是否能被非受控的介质或移动介质（不属于本机内部组成的驱动器或存储部件）启动？如能够启动，描述本医疗器械接受何种移动存储介质。

K) 在不借助工具的情况下，本医疗器械上能否安装未经制造商授权的软、硬件？

3.4.16 对操作者与管理员提供网络安全指导的能力 SGUD

制造商应回答下述问题，向责任方披露医疗器械的本项网络安全能力：

a) 对使用者是否提供医疗器械网络安全相关特性的文档？

b) 是否提供医疗器械、存储介质的数据去标识化指导（如何永久去除敏感数据的指导）？

3.4.17 存储保密能力 STCF

制造商应回答下述问题，向责任方披露医疗器械的本项网络安全能力：

a) 医疗器械是否利用闲置时间进行数据加密？

3.4.18 传输保密能力 TXCF

制造商应回答下述问题，向责任方披露医疗器械的本项网络安全能力：

a) 隐私数据的传输是否仅仅通过点对点的专线传输？

注：点对点的专线是指不能由外部人员接触到的系统布线，如：物理上受控的检查室、机房、控制柜、建筑的布线区域。

b) 在通过网络或者移动介质进行传输前，对隐私数据是否进行了加密？如有加密，注释说明加密机制所使用的标准。

c) 隐私数据的接收方，是否仅限于固定清单所列的范围？

3.4.19 保障数据传输完整性的能力 TXIG

制造商应回答下述问题，向责任方披露医疗器械的本项网络安全能力：

a) 医疗器械是否有确认传输数据未经篡改的机制？如有，注释说明此机制是如何实现的。

3.4.20 其它网络安全能力 OTHR

制造商应回答下述问题，向责任方披露医疗器械的本项网络安全能力：

a) 医疗器械是否支持远程维护？

b) 医疗器械是否可以对来自于或指向到特定的设备、用户、地址（如 IP 地址）的远程访问予以限制？

b.1) 医疗器械是否可以被配置为依赖本地用户来接受或发起远程访问？

3.5 信息披露的方式

制造商可在医疗器械随附技术资料中进行网络安全信息的披露。随附技术资料包含用户手册、服务维护指南以及安全、有效使用设备的其他相关技术文献。

经评估若在随附技术资料中公开披露网络安全信息存在信息泄漏的风险，本标准所规定的网络安全能力信息，也可以在责任方索取后予以提供。

注： 责任方向制造商索取相应信息时，制造商有义务将本标准所所规定的网络安全能力信息提供给责任方。无限制地公开网络安全能力信息是不可取的，相应的信息若被恶意破坏者获得，有可能被用来分析产品的网络安全脆弱性，为其快速地选定攻击目标，制定攻击策略提供便利。

参考文献

[1] 医疗器械网络安全注册技术审查指导原则，2017

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

[3] HIMSS/NEMA Standard HN 1-2013, Manufacturer Disclosure Statement for Medical Device Security.