**医疗器械网络安全管理的上市前申请内容**

**行业和美国食品药品监督管理局工作人员指南草案**

***指南草案***

**本指南草案文件仅供征求意见使用。**

**文件发布日期：2018年10月18日**

关于本文件草案的意见和建议应在《联邦公报》发布指南草案有效性通知后150天内提交。请提交电子意见至[https://www.regulations.gov](https://www.regulations.gov/)。可将书面意见提交至：美国食品药品监督管理局备案文件管理部（5630 Fishers Lane, rm. 1061, (HFA-305), Rockville, MD 20852）。所有意见均应注明《联邦公报》发布的备案文件编号。

如对本文件有任何疑问，请致电（301）796-6937或发送电子邮件至CyberMed@fda.hhs.gov联系中心主任办公室的Suzanne Schwartz。有关本文件中CBER监管器械的问题，请致电1-800-835-4709或240-402-8010联系交流、外联和发展办公室（OCOD）。

**本指南最终将取代2014年10月2日的《医疗器械网络安全管理的上市前申请内容-最终指南》**

**美国卫生与公众服务部**

**美国食品药品监督管理局**

**医疗器械和放射健康中心**

**生物制品评价和研究中心**

**前言**

**更多副本**

**医疗器械和放射健康中心（CDRH）**

更多副本可通过互联网获取。您也可以通过电子邮件发送请求至CDRH-Guidance@fda.hhs.gov获取本指南的副本。请在申请中提供文件编号GUD1825注明您所要求获取的指南。

**生物制品评价和研究中心（CBER）**

更多副本可通过以下途径获取：寄送信函至生物制品评价和研究中心（CBER）、交流、外联和发展办公室（OCOD），10903 New Hampshire Ave., Bldg 71, Room 3128, Silver Spring, MD 20993-0002；或致电1-800-835-4709或240-402-8010；或发送电子邮件至ocod@fda.hhs.gov或登录网址：<https://www.fda.gov/BiologicsBloodVaccines/GuidanceComplianceRegulatoryInformation/Guidances/default.htm>

**目录**

[I. 前言 4](#_Toc98749580)

[II. 范围 5](#_Toc98749581)

[III. 定义 6](#_Toc98749582)

[IV. 一般原则与风险评估 8](#_Toc98749583)

[V. 设计一个值得信赖的器械：NIST网络安全框架的应用 11](#_Toc98749584)

[VI. 对有网络安全风险的器械的标签建议 18](#_Toc98749585)

[VII. 网络安全文件 21](#_Toc98749586)

[VIII. 认可的标准 24](#_Toc98749587)

**医疗器械网络安全管理的上市前申请内容**

**行业和美国食品药品监督管理局工作人员指南草案**

本指南代表美国食品药品监督管理局（FDA）对该主题的当前看法。本文件不赋予任何人任何权利，对FDA或公众不具有约束力。如果替代方法满足适用的情形和法规的要求，则贵司可使用替代方法。如需讨论替代方法，请联系标题页所列负责本指南的FDA工作人员或办公室***。***

# I. 前言

随着无线设备、互联网和网络连接的设备、便携式媒体（如USB或CD）的使用越来越多，以及与医疗器械相关的健康信息的电子交换越来越频繁，因此确保医疗器械功能和安全的有效网络安全的需求变得更加重要。此外，医疗部门越来越频繁地面临更加严重的网络安全威胁，对临床的影响也更大。网络安全事件使医疗器械和医院网络无法运行，扰乱了美国和全球的医疗机构对患者的护理。这种网络攻击和漏洞可能会延迟诊断和/或治疗，并可能导致患者受到伤害。

该指南旨在向行业提供有关网络安全器械设计、标签以及FDA在有网络安全风险的器械上市前提交的文件申请建议。这些建议可以促进高效的上市前审查程序，并有助于确保上市的医疗器械对网络安全威胁有足够的抵御能力。

尽管FDA在2014年发布了说明上市前申请预期内容的最终指南，但随着快速发展的形势，以及行业对面临的威胁及其潜在缓解措施的进一步理解，需要一个更新的方法。该指南由FDA制定，目的是通过确定制造商在设计和开发其医疗器械以及为这些器械准备上市前申请时应处理的与网络安全有关的问题来协助行业。本指南文件中的建议旨在补充FDA的《医疗器械所含软件的上市前申请内容指南》[[1]](#footnote-0)和《行业指南：含有现成（OTS）软件的联网医疗器械的网络安全》[[2]](#footnote-1)本指南定稿后，将取代《医疗器械网络安全管理上市前申请内容》的最终指南。[[3]](#footnote-2)

对于本文件中引用的FDA公认标准的当前版本，请参见FDA公认共识标准数据库。[[4]](#footnote-3)

FDA指南文件，包括本指南，并未规定具有法律强制力的责任。相反，指南描述了FDA对该主题的当前看法，除非引用了具体监管或法定要求，否则应仅视为建议。FDA指南中使用的“应该（should）”一词指建议或推荐进行某一事项，并非强制要求。

# II. 范围

本指南提供了在FDA医疗器械上市前申请中应考虑的建议和信息，以实现有效的网络安全管理。有效的网络安全管理旨在通过减少器械的可利用性来降低伤害患者的风险，这种可利用性可能导致有意或无意地损害器械安全和基本性能。[[5]](#footnote-4)

本指南文件适用于以下包含软件（包括固件）或可编程逻辑的器械以及作为医疗器械的软件（统称为“软件器械”）的上市前申请。[[6]](#footnote-5)

• 上市前通知（510（k））申请，包括传统、特殊和简略申请。

• 新申请；

• 上市前批准申请（PMA）；

• 产品开发协议（PDP）；

• 人道主义器械豁免（HDE）申请。

# III. 定义

这里列出的定义旨在用于评估医疗器械网络安全的背景。

**资产**-任何对个人或组织有价值的东西。[[7]](#footnote-6)

**认证**-作为允许访问器械、其数据、信息或系统的先决条件，验证用户、进程或器械的身份的行为。[[8]](#footnote-7)

**真实性**-真实的、能够被验证和信任的属性；相信信息的内容来自预期的一方，并且在传输或存储过程中没有被修改。[[9]](#footnote-8)

**授权**-被授予访问器械资源的权利或许可。[[10]](#footnote-9)

**可及性**-以预期的方式及时获取和使用（即保证信息在需要时可以使用）的数据、信息和信息系统的属性。

**保密性**-数据、信息或系统结构的属性，只有被授权的人和实体才能访问，并在授权的时间以授权的方式进行处理，从而有助于确保数据和系统的安全。保密性保证未经授权的用户不能（即只有受信任的用户能够访问）访问数据、信息或系统结构。

**配置**-可以描述或安排器械或系统组件的可能条件、参数和规格。[[11]](#footnote-10)

**严格加密-**密码学权威人士认为的足够安全的密码算法、协议和实施。

**网络安全**-是防止未经授权的访问、修改、滥用或拒绝使用，或未经授权使用存储、访问或从医疗器械转移到外部接收者的信息的过程。

**网络安全材料清单（CBOM）**-包括但不限于商业、开放源码和现成的软件和硬件组件的清单，这些组件容易或可能受到漏洞的影响。

**拒绝服务** - 阻止系统按照预定目的运作的行为。设备或实体可能无法运作，或被迫在降级状态下运作；依赖及时性的运作可能会延迟。[[12]](#footnote-11)

**加密**-对数据进行加密改造，使之成为掩盖数据原意的形式，以防数据泄露或使用。[[13]](#footnote-12)

**支持结束** - 产品制造商停止为产品或服务提供支持的时间点，其中可能包括网络安全支持。

**完整性** - 数据、信息和软件的属性是准确和完整的，避免修改不当。

**抖动**-数据包的延迟差异，与排队有关。[[14]](#footnote-13)

**生命周期**-医疗器械生命周期中的所有阶段，从最初的构想到最后的报废和处理。[[15]](#footnote-14)

**恶意软件** - 恶意设计的软件，旨在破坏正常功能，收集敏感信息和/或访问其他连接系统。

**可修补性/可更新性** - 器械和相关系统及时更新和修补的难易程度。

**患者伤害**-患者的身体伤害或健康损害，包括死亡。[[16]](#footnote-15)器械的网络安全漏洞（如真实性、可及性、完整性或保密性的丧失）可能对健康构成风险，并可能导致患者受到伤害。

**特权用户**-被授权（同时也被信任）执行普通用户无权执行的安全相关功能的用户。[[17]](#footnote-16)

**服务质量**-网络服务可测量的端到端性能属性，可由终端用户和服务提供商之间的服务水平协议事先保证，以满足特定的客户应用要求。[[18]](#footnote-17)

**风险**-损害发生的概率和该损害的严重程度的组合。[[19]](#footnote-18)

**风险分析**-系统地利用现有的信息来识别危险并估计风险。19

**值得信赖的器械**-包含硬件、软件和/或可编程逻辑的医疗器械，该器械具有以下特点：（1）合理防止网络安全入侵和滥用；（2）提供适当范围的可及性、可靠性和正确操作；（3）在合理范围内适合执行其预期功能；（4）遵守公认的安全程序。[[20]](#footnote-19)

# IV. 一般原则与风险评估

为了证明软件器械的安全性和有效性的合理保证，与质量体系条例（QSR）（21 CFR第820部分）的要求相关的文件通常是上市前申请的必要部分。另请参见《医疗器械所含软件的上市前申请内容指南》（可访问<https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm089593.pdf>）。作为QSR设计控制的一部分，制造商必须“建立和保持确认器械设计的程序，”其中“应在适当的时候包括软件确认和风险分析。”21 CFR 820.30（g）。

作为21 CFR 820.30（g）要求的软件确认和风险分析的一部分，软件器械制造商可能需要酌情建立网络安全漏洞和管理方法。FDA建议这种方法应包括网络安全设计控制，以确保医疗器械的网络安全，维护医疗器械的安全性和有效性。这样的设计控制可能使FDA更大程度发现您的器械符合其适用的法定标准，从而进行上市前审查。[[21]](#footnote-20)

FDA认识到，保证医疗器械的安全性是利益相关者的共同责任，其中包括医疗机构、患者、医疗服务提供者和医疗器械制造商。未能维护网络安全可能导致器械功能受损，数据（医疗或个人）的真实性、可及性或完整性丢失，或使其他连接器械或网络受到安全威胁。这反过来又有可能导致患者生病、受伤或死亡。

本指南中的建议旨在帮助制造商：

1) 采用基于风险的方法来设计和开发具有适当网络安全保护的医疗器械。

2) 通过评估产品整个生命周期的风险和缓解措施，对器械网络安全采取全面的方法。

3) 确保关键器械安全和基本性能的维护和连续性[[22]](#footnote-21)；

4) 促进值得信赖的器械的发展，以帮助确保器械的持续安全和有效。

QSR要求用计算机软件实现自动化的器械制造商建立和维护程序，以确保与器械有关的设计要求是合理的，并落实器械的预期用途，包括用户和患者的需要。21 CFR 820.30（c）。FDA建议制造商在设计和开发医疗器械的过程中考虑以下内容，以解决网络安全问题：

• 识别资产、威胁和脆弱性

• 评估威胁和漏洞对器械功能和终端用户/患者的影响；

• 评估威胁的可能性[[23]](#footnote-22)和漏洞被利用的可能性；

• 确定风险水平和适当的缓解策略；

• 评估剩余风险和风险接受标准。

能够（通过无线或硬接线）与另一器械、互联网或其他网络、或与便携式媒体（如USB或CD）连接的医疗器械比没有连接的器械更容易受到网络安全威胁。制造商在确定适合器械的设计特点和网络安全复原力水平时，应采用基于风险的方法。所以网络安全材料清单（CBOM）可以成为识别资产、威胁和责任的一个关键因素。利用CBOM也可以支持遵守采购控制（21 CFR 820.50），通过促进建立关于所有购买或以其他方式收到的产品的网络安全的要求。需要安全控制的程度将取决于器械的预期用途、其电子数据接口的存在和功能、预期的使用环境、存在的网络安全漏洞的类型、漏洞的可利用性（有意还是无意）以及由于网络安全漏洞而对患者造成伤害风险的可能性。

为了本指南的目的，并帮助澄清FDA的上市前网络安全建议，我们根据器械的网络安全风险定义了两个“层级”：

**第1级“较高的网络安全风险”**

如果符合以下标准，为一级器械：

1) 该器械能够（例如，采用有线、无线方式）连接到另一个医疗或非医疗产品，或连接到一个网络，或连接到互联网；

2) 影响器械的网络安全事件可能直接导致多个患者受到伤害。

一级器械包括但不限于：植入式心律转复除颤器（ICD）、心脏起搏器、左心室辅助器械（LVAD）、脑刺激器和神经刺激器、透析器械、输液泵和胰岛素泵，以及与这些器械互动的配套连接系统，如家用监视器和具有指令和控制功能的系统，如程序器。

**第2级“标准网络安全风险”**

不符合一级器械标准的医疗器械。

仅就本网络安全指南而言，FDA引入了较高和标准的网络安全风险等级，以帮助医疗器械制造商设计安全的器械并协助向FDA提供证明文件。我们认识到，这种网络安全风险分级可能与FDA现有的法定器械分类不相吻合。例如，根据制造商的评估和器械设计，II类器械（如输液泵）可能符合一级较高网络安全风险的标准，而III类器械（如无网络连接的冠状动脉切除器械）可能符合二级标准网络安全风险的标准。本指南中描述的原则和方法广泛适用于所有医疗器械，旨在与美国国家标准与技术研究所（NIST）“改善关键基础设施网络安全的框架”保持一致，通过关注识别、保护、检测、响应和恢复等核心功能来管理网络安全相关风险。[[24]](#footnote-23)

# V. 设计一个值得信赖的器械：NIST网络安全框架的应用

如第IV节所述，对于软件器械，与设计控制有关的文件往往是必要的提交资料，特别是21 CFR 820.30（g）中的设计确认和软件确认和风险分析，这些文件可以在上市前申请中提供安全和有效性的合理保证。对于有网络安全风险的器械，我们建议制造商设计出值得信赖的器械，因为这更有可能满足其适用的法定标准进行上市前审查，也因为值得信赖的器械更有可能在整个生命周期内保持安全和有效。值得信赖的器械可以：（1）合理地防止网络安全入侵和滥用；（2）提供适当范围的可及性、可靠性和正确操作；（3）在合理范围内执行其预期功能；（4）遵守公认的安全程序。此外，证明器械可靠性的文件将帮助FDA更快速、有效地评估器械在网络安全方面的安全性和有效性。

本节介绍了FDA认为在值得信赖的器械的设计中应包括的具体设计特征和网络安全设计控制。我们建议具有较高网络安全风险的一级器械的上市前申请中的文件可以证明器械设计和风险评估纳入下述网络安全设计控制的过程。对于具有标准网络安全风险的二级器械，我们建议制造商在其上市前申请的文件中包括：1）证明已经纳入了本节所述的每个具体设计特征和网络安全设计控制，2）提供基于风险的理由，说明本节所述的具体网络安全设计控制为什么不合适。基于风险的理由应该利用对可利用性的分析来描述可能性而不是概率。

提交的文件包括证明本文件中可能没有描述的可比性和/或额外的网络安全设计控制。此外，由于网络安全设计控制在开发阶段的早期建立，我们建议业界利用FDA预提交流程来讨论设计考虑事项，以满足整个器械生命周期内网络安全风险管理的充分性。[[25]](#footnote-24)

## A. 识别和保护器械资产和功能

制造商应设计出值得信赖的器械，并在上市前审查中提供文件以证明其器械的可靠性。特别是，器械和系统的设计应能保护资产和功能，以减少因失去真实性、可及性、完整性和保密性而造成的多患者伤害的风险。具体来说，保护机制应防止所有未经授权的使用（通过所有接口）；确保代码、数据和执行的完整性（颠覆系统功能/安全/保障功能）；并酌情保护数据的保密性（只要其释放可能被利用来实现对多患者的伤害。作为上市前提交文件的一部分，制造商应提交文件，证明如何满足这些设计期望。

### 1 防止未经授权使用

为了减少因失去真实性、可及性、完整性和保密性而造成的多患者伤害的风险，我们在以下部分提供了有关认证、授权和加密的设计建议。认证是用来防止未经授权访问器械功能和防止未经授权的软件执行。它提供了通信和/或命令是未经修改的，并且来自授权的来源这一保证，这与其他防止复制的控制相结合，使外部对手更难以向安全关键系统发出潜在的有害命令。通常情况下，授权只能作为一种安全控制，与正确实施的认证结合起来才有效。除非在系统设计特征内在地提供同等或更强的保证的情况下，所有器械都应适当地认证潜在的有害命令和/或数据。

作为一种防御措施，授权会强制执行与认证凭证和/或角色相关的权限，以拒绝所有不允许的行为。这意味着，使用权限较低的凭证的对手不应该能够访问需要较高权限的器械资源或功能（即，默认的器械设计应该防止这种情况发生）。器械应该有适当的保护措施，防止敏感信息在存储或传输过程中被未经授权的各方读取。酌情使用加密技术可以保护敏感信息不被未经授权的披露。以下概述提供了认证、授权和加密的推荐设计的实现方法：

**(a) 只对受信任的用户和器械进行访问限制**

(i) 通过对用户的认证（例如，用户ID和密码、智能卡、生物识别）限制对器械的访问。

(ii) 在适合环境情况下，使用自动定时的方法来终止系统内的会话。

(iii) 采用分层授权模式，根据用户角色（例如，护理人员、患者、保健提供者、系统管理员）或器械功能区分权限。

(iv) 使用适当的认证（例如，多因素认证，允许系统管理员、服务技术人员、维护人员访问特权器械）。

(v) 加强密码保护。不要使用硬编码的、默认的、容易猜测的、容易泄露的凭证（即，每个器械的密码都是一样的；不可更改；可以持续默认；难以更改；容易被公开披露）。对用于特权器械访问的密码限制访问。

(vi) 考虑对器械及其通信端口进行物理锁定，以尽量减少篡改。

(b) **认证和检查安全关键命令的授权情况**

(i) 使用认证来防止未经授权访问器械功能，并防止未经授权（任意）执行软件。

(ii) 在允许软件或固件更新之前要求用户认证，包括那些影响操作系统、应用程序和反恶意软件的更新。

(iii) 使用驻留在器械上的加强认证对人员、消息、命令以及所有其他通信路径（如适用）进行认证。

(iv) 认证所有外部连接。例如，如果一个器械连接到一个异地服务器，则其和服务器应该相互验证，即使连接是通过一个或多个现有的可信通道启动。

(v) 认证固件和软件。验证软件/固件内容、版本号和其他元数据的认证标签（例如，签名、消息认证码（MAC））。拟安装的版本号本身应该是有签名/MAC的。对授权用户来说，器械应可以电子识别（例如，型号、序列号）。

(vi) 根据认证凭证或其他不可辩驳的证据进行授权检查。例如，医疗器械的程序员应具有基于加密认证或意图信号授予的提升权限，这些信号不能由另一个器械（如家用监视器）以基于软件的攻击方式实际产生。

(vii) 器械应被设计成“默认拒绝”，即器械未明确允许的，默认为拒绝。例如，器械一般应拒绝所有未经授权的连接（例如，传入的TCP、USB、蓝牙、串行连接）。

(viii) 应适用最小特权原则，只允许执行一项功能所需的访问水平。

### 2. 通过保持代码、数据和执行的完整性来确保受信任的内容

#### (a) 代码完整性

(i) 只允许安装经加密验证的固件/软件更新。使用加密签名的更新，通过确保新的更新比当前安装的版本更新，帮助防止未经授权降低保护水平（降级或回滚攻击）。

(ii) 在可行的情况下，确保软件的完整性在执行前得到验证，例如，基于数字签名的“白名单”。

#### (b) 数据完整性

(i) 验证所有传入数据的完整性（确保其在传输过程中或静态下未被修改，并且其格式良好/符合预期的协议/规范）。

(ii) 确保与器械之间的安全数据传输能力，并在适当的时候，使用加密和认证数据传输的终端的方法。

(iii) 保护必要数据的完整性，以确保器械的安全和基本性能。

(iv) 使用当前NIST推荐的密码学标准（例如，FIPS 140-2，NIST[[26]](#footnote-25) B套件[[27]](#footnote-26)），或同等强度的通信通道密码保护。

(v) 使用每个器械唯一的加密安全通信密钥，以防止利用一个密钥的知识来访问众多的器械。

#### (c) 执行完整性

在可行的情况下，使用行业公认的最佳实践来维护/验证代码的完整性，同时在器械上执行。

### 3. 保持数据的保密性

制造商应确保任何/所有数据的保密性，这些数据的披露可能导致患者受到伤害（例如，通过使用证书、加密）。凭证保密性丧失可能被威胁者利用，以实现对多个患者的伤害。缺乏对“静态”和“传输”中的敏感信息的加密保护，会使这些信息被滥用，从而导致患者受到伤害。

其他伤害，如丢失受保护的机密健康信息（PHI），在本指南中不被视为“患者伤害”。虽然保护PHI的保密性不在本文件的范围内，但应注意，根据适用的联邦和州法律，包括《健康保险便携性和责任法案》（HIPAA），制造商和/或其他实体可能有义务在整个产品生命周期内保护PHI的保密性、完整性和可及性。[[28]](#footnote-27)

## B. 检测、响应、恢复：设计期望

正确的器械设计可以大大降低器械在市场上和使用环境中部署时的网络安全风险。因此，适当的设计应预见到检测和应对动态网络安全风险的需要，包括部署网络安全常规更新和补丁以及紧急变通的需要。以下项目阐述了对值得信赖的器械的设计建议，因为它涉及到NIST的核心功能-检测、响应和恢复。

### 1. 设计器械，及时检测网络安全事件

（a） 实现设计功能，允许在正常使用期间对安全损害进行检测、识别、记录、计时和采取行动。

（b） 器械的设计应允许常规的安全和防病毒扫描，使器械的安全和基本性能不受影响。

（c） 确保设计能够捕获法庭证据。设计应包括为安全事件创建和存储日志文件的机制。文件应包括日志文件如何以及在哪里被定位、存储、回收、归档，以及如何被自动分析软件（如入侵检测系统，IDS）所消耗。其中安全事件包括但不限于配置变化、网络异常、登录尝试和异常流量（例如，向未知实体发送请求）。

（d） 器械设计应通过指定安全配置来限制漏洞的潜在影响。安全配置可包括终端保护，如反恶意软件、防火墙/防火墙规则、白名单、定义安全事件参数、日志参数、物理安全检测。

（e） 器械设计应能实现软件配置管理，并允许跟踪和控制软件的变化，使授权用户能够以电子方式获得（即机器可读）。

（f） 产品的生命周期，包括其设计，应有助于对某一漏洞进行跨器械型号和产品系列的变体分析。

（g） 器械设计应提供机器可读的电子格式的CBOM，以便自动消耗。[[29]](#footnote-28)

### 2. 设计器械应对和控制潜在网络安全事件的影响

（a） 器械应在发现潜在的网络安全漏洞时通知用户。

（b） 器械应能预测到对软件补丁和更新的需要，以解决未来的网络安全漏洞。

（c） 器械应有利于快速确认、验证和测试补丁和更新。

（d） 设计架构应有利于快速部署补丁和更新。

### 3. 设计器械恢复因网络安全事件而受损的能力或服务

（a） 实施保护关键功能和数据的设备功能，即使在器械的网络安全已被破坏的情况下。

（b） 设计应提供由经过认证的特权用户保留和恢复器械配置的方法。

（c） 设计应规定当系统的任何组成部分与系统其他部分的通信能力被中断时（包括持续时间较长的中断），系统的任何组件拥有的自主功能（复原力）的水平。

（d） 器械的设计应能适应可能的网络安全事件情况，如网络中断、拒绝服务攻击、其他产品过度使用带宽、服务质量（QoS）中断和过度抖动（即接收数据包的延迟变化）。

# VI. 对有网络安全风险的器械的标签建议

本节介绍了一些器械标签要求和法规的背景，并解释了标签对具有网络安全风险的器械的安全性和有效性可能起到的作用。然后，它包含了向最终用户传达相关安全信息的标签建议，这可能有助于制造商遵守适用的要求，并有助于确保器械在其整个生命周期内保持安全和有效。

FDA以多种方式对器械标签进行管理。例如，《FD&C法案》第502（f）条要求标签包括充分的使用说明。根据《FD&C法案》第502（a）（1）条，如果医疗器械的标签在任何方面都是虚假的或具有误导性，则被视为贴标错误。根据第201（n）条，如果标签没有揭示在标签规定的使用条件下或在习惯或通常的使用条件下使用该物品可能产生的后果的重要事实，则标签可能具有误导性。另请参见21 CFR 1.21。

FDA的器械条例包含与标签有关的进一步要求。例如，21 CFR 801.5要求标签包括充分的使用说明，其中包含该器械的所有条件、目的或用途的声明（例如，危险、警告、预防措施、禁忌证）。对于处方药，21 CFR 801.109（c）要求标签包括任何相关的危险、禁忌证、副作用和预防措施，在此基础上，依法获准使用该药的医生可以安全地使用该药并达到预期的目的。

对于有网络安全风险的器械，将相关安全信息告知最终用户可能是遵守标签要求的有效方式。FDA还认为，通过标签告知最终用户安全信息可能是QSR设计控制的一个重要部分，有助于减轻网络安全风险，有助于确保器械的持续安全和有效。因此，在起草纳入上市前提交申请的标签时，制造商应考虑所有适用的标签要求，以及通过标签告知用户可能是管理网络安全风险的有效方式。具体而言，我们建议在标签中加入以下内容，以便向最终用户传达相关的安全信息：[[30]](#footnote-29)

1. 与适合预期使用环境的建议网络安全控制有关的器械说明和产品规格（例如，安装反病毒软件，使用防火墙）。

2. 对保护关键功能的器械特征的描述，包括在器械的网络安全遭到破坏的情况下。

3. 关于备份和恢复功能的描述，以及恢复配置的程序。

4. 向用户提供有关支持性基础设施要求的具体指导，以便器械能够按预期运行。

5. 关于器械如何使用安全配置或可以使用安全配置进行加固的描述。安全配置可包括终端保护，如反恶意软件、防火墙/防火墙规则、白名单、安全事件参数、日志参数、物理安全检测。

6. 预计接收和/或发送数据的网络端口和其他接口的列表，以及对端口功能的描述，以及端口是传入还是传出（注意，未使用的端口应被禁用）。

7. 对授权用户从制造商处下载可识别版本的软件和固件的系统程序的描述。

8. 描述设计如何使器械在检测到异常情况（即安全事件）时宣布。安全事件类型可以是配置变化、网络异常、登录尝试、异常流量（例如，向未知实体发送请求）。

9. 关于如何获取法庭证据的描述，包括但不限于为安全事件保留的任何日志文件。日志文件的描述应包括日志文件如何以及在哪里被定位、存储、回收、归档，以及如何被自动分析软件（如入侵检测系统，IDS）消耗。

10. 对经过认证的特权用户保留和恢复器械配置的方法的描述。

11. 为终端用户提供足够详细的系统图。

12. CBOM包括但不限于商业、开放源码和现成的软件和硬件组件清单，以使器械用户（包括患者、提供者和医疗服务组织（HDO））有效地管理其资产，了解已识别的漏洞对器械（和连接系统）的潜在影响，并部署应对措施以保持器械的基本性能。

13. 在适当的情况下，允许安全网络（连接）部署和服务的技术指示，以及对用户在发现网络安全漏洞或事件时如何应对的指示。

14. 有关器械网络安全的支持结束的信息（已知情况下）。在支持结束时，制造商可能不再能够合理地提供安全补丁或软件更新。如果器械在支持结束后仍在使用，可以预计最终用户的网络安全风险会随着时间的推移而增加。

这些建议旨在向最终用户传达相关的安全信息，从而帮助确保器械在其生命周期内保持安全和有效。

# VII. 网络安全文件

本节列出了制造商在其上市前申请中应提交的建议文件，以及任何提交的软件文件[[31]](#footnote-30)。具体而言，FDA建议制造商包括上述第五节的设计特点的文件，以及风险管理文件和标签，以证明基于风险的方法，其中包括设计特点和适合器械的网络安全复原力水平。

## A. 设计文件

设计文件应证明器械值得信赖。

1. 对于一级器械，要有第V节中每项建议的文件。

2. 对于二级器械，应提供针对第V节中每项建议的文件，或包括基于风险的理由，说明没有必要进行网络安全设计控制的原因。基于风险的理由应该利用对可利用性的分析来描述可能性而不是概率。

3. 系统图，其详细程度足以让人了解具体的器械设计元素（来自第V节）是如何被纳入系统级和整体的，对整个系统的分析是必要的，以了解制造商的威胁模型和更大的生态系统中的器械。

**系统图应包括：**

（a） 网络图、架构图、流程图和状态图。

（b） 接口、组件、资产、沟通途径、协议和网络端口。

（c） 系统中每个通信资产或组件的认证机制和控制，包括网站、服务器、互操作系统、云存储等。

（d） 如果用户与这些资产或通信渠道互动，则包括他们的角色和责任水平。

（e） 加密方法的使用应包括对所使用的方法和加密密钥使用的类型和水平的描述，以及它们在整个系统中的使用风格（一次性使用、密钥长度、采用的标准、对称或其他，等等）。说明中还应包括对固件和软件更新的加密保护细节。

4. 描述设计特点的总结，允许在医疗器械的整个生命周期内根据需要进行有效的软件更新和修补，以继续确保其安全性和有效性。[[32]](#footnote-31)

## B. 风险管理文件

风险评估将设计与威胁模型、临床危害、缓解措施和测试联系起来。建立一个安全的设计架构至关重要，这样可以充分地管理风险。建议的文件利用了技术信息报告AAMI TIR57医疗器械安全风险管理原则中描述的安全风险管理报告的概念， [[33]](#footnote-32)但包含相同或类似信息的其他形式的文件也可以接受。安全风险管理报告是一种全面的方法，它以一种有意义的方式考虑了保密安全和安全风险分析。它提供了一个评价、评估和缓解活动的总结，以确保器械的合理安全。以下建议涉及到值得信赖的器械的风险管理报告中的预期内容。

1. 系统级的威胁模型，包括对系统级风险的考虑，包括但不限于与供应链（例如，确保器械没有恶意软件）、设计、生产和部署（即，进入连接/联网环境）有关的风险。

2. 器械设计中考虑的所有网络安全风险的具体清单。我们建议提供对风险的描述，利用对可利用性的分析来描述可能性而不是概率。如果提供数字概率，我们建议提供附加信息，解释概率计算的过程。

3. 为器械建立的所有网络安全控制的具体清单和理由。这应该包括所有与器械相关的有意和无意的网络安全风险有关的风险缓解措施和设计考虑，包括：

(a） 与访问控制、加密/解密、防火墙、入侵检测/预防、防病毒包等有关的可核实的功能/子系统要求清单。

(b） 影响其他功能、数据和接口要求的安全要求的可核查清单。

4. 描述为确保网络安全风险控制的充分性而进行的测试（例如，在执行规定的安全政策方面的安全有效性、所需流量条件的性能、稳定性和可靠性（视情况而定）。测试报告应包括：

(a) 器械性能的测试

(b) 系统中第三方OTS软件的安全有效性证据。

(c) 静态和动态代码分析，包括测试“硬编码”、默认、容易猜测和容易泄露的凭证。

(d) 漏洞扫描

(e) 稳健性测试

(f) 边界分析

(g) 渗透测试

(h) 第三方测试报告

5. 可追溯性矩阵将实际网络安全控制与您的安全风险和危险分析中所考虑的网络安全风险联系起来。

6. 与国家漏洞数据库（NVD）或类似的已知漏洞数据库交叉引用的CBOM。提供解决已知漏洞的标准和不解决其余已知漏洞的理由，与FDA的最终指南《医疗器械网络安全的上市后管理》一致。[[34]](#footnote-33)

FDA认为，提供像上述建议的网络安全文件将有助于FDA发现您的器械是否符合其适用的上市前审查法定标准。

# VIII. 认可的标准

请参考FDA的网站，了解迄今为止FDA认可的关于信息技术（IT）和医疗器械安全性的共识标准的最新清单。

关于FDA认可的共识标准的最新清单，建议您参考[FDA认可的共识标准数据库](http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfStandards/search.cfm)，[[35]](#footnote-34)并在标题搜索中输入“安全”，以获得FDA认可的信息技术和医疗器械安全共识标准的最新清单。

关于共识标准认可的信息，请参见指南文件[《CDRH识别和评估候选共识标准的标准操作程序》](https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077322)[[36]](#footnote-35)

关于在上市前申请中使用标准的信息，参见指南文件[《在医疗器械上市前申请中适当使用自愿共识标准》](https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077295.pdf)[[37]](#footnote-36)



1. <https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM089593> [↑](#footnote-ref-0)
2. <https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM077823> [↑](#footnote-ref-1)
3. <https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190> [↑](#footnote-ref-2)
4. 访问<https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfStandards/search.cfm> [↑](#footnote-ref-3)
5. ANSI/AAMI ES60601-1:2005/（（R）2012和A1:2012、C1:2009/（R）2012和A2:2010/（R）2012（合并文本）医用电气设备-第1部分：基本安全和基本性能的一般要求（IEC 60601-1:2005，MOD），第3.27节将“基本性能”定义为“除与基本安全有关的临床功能的性能，如果损失或退化超过制造商规定的限度会导致不可接受的风险” [↑](#footnote-ref-4)
6. 制造商也可以考虑将本指南中描述的网络安全原则酌情应用于临床试验用器械豁免申请和免于上市前审查的器械。 [↑](#footnote-ref-5)
7. 如ISO/IEC 27032《信息技术-安全技术-网络安全指南》所定义。 [↑](#footnote-ref-6)
8. 改编自NIST FIPS 200 联邦信息和信息系统的最低安全要求。认证的定义是验证用户、进程或器械的身份，通常作为允许访问信息系统中的资源的先决条件。 [↑](#footnote-ref-7)
9. 来自NIST SP 800-53 联邦信息系统和组织的安全和隐私控制：真实性被定义为真实的、能够被验证和信任的属性；对传输、信息或信息申办方的有效性的信心。参见认证一条。 [↑](#footnote-ref-8)
10. 改编自NISTIR 7298《关键信息安全术语》：授权指授予用户、程序或进程的访问权限或授予这些权限的行为。 [↑](#footnote-ref-9)
11. 改编自NIST SP 800-128《以安全为重点的信息系统配置管理指南》：配置指可以描述或安排一个信息系统或系统组件的可能条件、参数和规格。 [↑](#footnote-ref-10)
12. 来自NIST SP 800-24 PBX漏洞分析：率先找到您的PBX中的漏洞。 [↑](#footnote-ref-11)
13. 来自NIST SP 800-82《行业控制系统（ICS）安全指南》。将数据（称为“明文”）加密转化为一种形式（称为“密文”），隐藏数据的原始含义，以防止其被获知或使用。如果转换可逆，则相应的逆转过程被称为“解密”，它是一种将加密数据恢复到原始状态的转换。 [↑](#footnote-ref-12)
14. 来自NIST SP 800-127《WiMAX无线通信安全指南》。 [↑](#footnote-ref-13)
15. ANSI/AAMI/ISO 14971医疗器械-风险管理在医疗器械中的应用 [↑](#footnote-ref-14)
16. ANSI/AAMI/ISO 14971医疗器械-风险管理在医疗器械中的应用将“*伤害”定义*为对人的健康的物理伤害或损害，或对财产或环境的损害。 [↑](#footnote-ref-15)
17. 来自NIST SP 800-53《联邦信息系统和组织的安全和隐私控制》 [↑](#footnote-ref-16)
18. 来自CNSSI 4009国家安全系统委员会（CNSS）的术语。 [↑](#footnote-ref-17)
19. ANSI/AAMI/ISO 14971医疗器械-风险管理在医疗器械中的应用 [↑](#footnote-ref-18)
20. 改编自NIST SP 800-32《公钥技术和联邦PKI基础设施介绍》，其中对可信系统的定义是：计算机硬件、软件和程序：（1）具有合理的安全性，防止入侵和滥用；（2）提供合理水平的可及性、可靠性和正确的操作；（3）合理地适合执行其预期功能；以及（4）遵守普遍接受的安全程序。 [↑](#footnote-ref-19)
21. 关于FDA如何评估510（k）申请中实质等同性的更多信息，请参见FDA指南文件[《510（k）计划：评估上市前通知中的实质等同[510（k）]》](https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM284443) [↑](#footnote-ref-20)
22. [医疗器械网络安全的售后管理](https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf)https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf [↑](#footnote-ref-21)
23. 可能性评估应利用对可利用性的分析，而不是概率。 [↑](#footnote-ref-22)
24. 美国国家标准与技术研究所（NIST）改善关键基础设施网络安全的框架，可访问<https://www.nist.gov/cyberframework> [↑](#footnote-ref-23)
25. 更多信息，请参见FDA的指南，《医疗器械申请的反馈请求：预申请计划和与美国食品药品监督管理局工作人员的会议》（<https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm311176.pdf>） [↑](#footnote-ref-24)
26. NIST FIPS 140-2加密模块验证计划可在以下网站获得：<https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Standards> [↑](#footnote-ref-25)
27. NIST FIPS 140-2 Suite B可在以下网站获得：<https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp2851.pdf> [↑](#footnote-ref-26)
28. HHS民权办公室执行《健康保险便携性和责任法案》（HIPAA）隐私规则，该规则保护承保实体或其商业伙伴创建、接收、维护或传输的个人可识别健康信息的隐私；HIPAA安全规则，该规则为电子受保护健康信息的安全制定国家标准；HIPAA违规通知规则，该规则要求承保实体和商业伙伴在不安全的受保护健康信息被泄露后提供通知；以及患者安全规则的保密规定，该规则保护用于分析患者安全事件和改善患者安全的可识别信息。参见健康信息隐私：http://www.hhs.gov/ocr/privacy/index.html。 [↑](#footnote-ref-27)
29. 卫生保健行业和网络安全工作组（HCIC TF）关于改善卫生保健行业网络安全的报告中的建议2.2，可访问https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf [↑](#footnote-ref-28)
30. 更多信息请参见IEC TR 80001-2-2和IEC TR 80001-2-8以及IEC TR 80001-2-9 [↑](#footnote-ref-29)
31. [医疗器械所含软件的上市前申请内容https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM089593](https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM089593)。 [↑](#footnote-ref-30)
32. 更多关于FDA对上市和分销器械的上市后网络安全漏洞管理的建议，参见[医疗器械网络安全的上市后管理https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf](https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf)。 [↑](#footnote-ref-31)
33. AAMI TIR57：医疗器械安全的原则-风险管理 [↑](#footnote-ref-32)
34. 这项活动将支持遵守采购控制（21 CFR 820.50），确保所有购买或以其他方式获得的产品和服务符合有关网络安全的特定要求。同样，这项活动将支持遵守设计控制和设计确认（21 CFR 820.30（g）），以帮助确保器械符合确定的用户需求和预期用途，包括确保器械的软件和硬件没有不可接受的网络安全漏洞。 [↑](#footnote-ref-33)
35. <https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfStandards/search.cfm> [↑](#footnote-ref-34)
36. <https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077322> [↑](#footnote-ref-35)
37. <https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077295.pdf> [↑](#footnote-ref-36)