网络安全 22 项解读

1.自动注销(ALOF-AUTOMATIC LOGOFF):产品在无人值守期间阻止非授权用户访问和使用的能力。

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。

■ 防止设备 无人照看时被入侵的能力

当预设时间段内医疗器械无人操作时，配置医疗器械，使其自动登出，若需要继续使用，可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;
- 无人操作的预设时间段可由用户或管理员进行配置;
- 系统自动锁定后，可由用户手工解锁。

2.审核(AUDIT CONTROLS-AUDT):产品提供用户活动可被审核的能力。

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。

■ 保留审核踪迹的能力(网络行为处于监控下)

保留审核总计，可以记录如下时间：

- 登入、登出信息;
- 隐私数据被显示、打印或以其他方式呈现;
- 数据的增、改、删;
- 基于移动存储介质的数据导入，导出;
- 基于外部连接(如网络连接)的数据导入，导出;
- 医疗器械的远程维护。

3.授权(AUTHORIZATION-AUTH):产品确定用户已获授权的能力。

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。

- 确定用户授权的能力
  - 医疗器械具有用户登入或其他措施，防止未经授权的用户进入
    - ✓ 可采取技术的措施:口、生物认证、钥匙卡等
  - 医疗器械区分用户身份给予不同的权限
    - ✓ 可设置权限如: 访客、日常用户、高级用户、管理员等。
  - 避免使医疗器械的拥护者、操作者获得不受限制的权限。
    - ✓ 如:通过管理员账号，或者通过获取权限的方式进入操作系统或应用程序。

4.节点鉴别(NODEAUTHENTICATION-NAUT):产品鉴别网络节点的能力。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。

- 通讯节点的验证能力
  - 医疗器械可提供或支持某种节点身份验证措施
  - 确保数据的发送与接收方互相识别并授权进行数据传输。

5.人员鉴别(PAUT-PERSONAUTHENTICATION):产品鉴别授权用户的能力。

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。

- 器械对使用者身份进行验证的能力
  - 可支持“用户名/密码”机制
  - 对密码强度的要求
  - 对密码给出时间限制
  - 避免多人共用一个用户名
  - 防止密码尝试活动
  - 初始密码在安装时、或者安装前修改
- 也可支持第三方身份验证机制。

6.连通性(CONN):产品保证连通网络安全可控的能力。

医疗器械能提供适宜的网络接口和医疗器械电子接口，以满足网络安全的需

求。

■ 网络接口:

医疗器械可通过网络接口(含转接接口)进行电子数据交换或远程访问与控制，此时需考虑网络的技术特征要求，包括但不限于网络形式(有线、无线)、网络类型(如广域网、局域网、个域网)、接口形式(如电口、光口)、数据接口(此时即数据协议，含标准协议、私有协议)、远程访问与控制方式(实时、非实时)、性能指标(如端口、传输速率、带宽)等。

无线网络包括 Wi-Fi(IEEE 802.11)、蓝牙 EEE 802.15)、射频、红外 4G/5G 等形式，其中医用无线专用设备(即未采用通用无线通信技术的医疗器械)应符合中国无线电管理相关规定。标准协议即业内公认标准所规范的数据传输协议，如 DICOM、HL7 等，需考虑其定制化功能的兼容性问题，私有协议需考虑兼容性问题。远程访问与控制亦包括操作系统软件所提供的远程会话或远程桌面功能。

■ 电子数据接口:

电子数据交换接口是指基于非网络的电子接口。医疗器械可通过非网络接口的其他电子接口 (如串口并口、USB 口、视频接口、音频接口，含调试接口、转接接口)或存储媒介 (如光盘、移动硬盘、U 盘)进行电子数据交换。此时需考虑其他电子接口或数据存储的技术特征要求。

其他电子接口可参照网络接口明确其技术特征要求。数据存储的技术特征要求包括但不限于存储媒介形式、数据接口(此时即文件存储格式，含标准格式、私有格式)、数据压缩方式(有损、无损)性能指标(如传输速率、容量等。标准格式即业内公认标准所规范的文件存储格式，如 JPEG、PNG 等，需考虑其文件格式完整性问题;私有格式需考虑兼容性问题。

7.物理防护(PHYSICAL LOCKSON DEVICE-PLOK):产品提供防止非授权用户访问和使用的物理防护措施的能力。

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。

■ 防范直接从存储截至上获取数据的能力

- 医疗器械所遗憾的隐私数据，在物理上提供保障吗?存储介质需要使用工

具才能去除。

- ✓ 技术方式/物理方式禁用所有接口管理措施禁止非授权人员接触器械器械/主机不能轻易的被打开密码锁。

8.系统加固(SYSTEM AND APPLICATION HARDENING-SAHD):产品通过固化措施对网络攻击和恶意软件的抵御能力。

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。

■ 强化器械内在的抗攻击能力

- ➢ 确保用于安装/升级的软件都是经制造商授权
- ➢ 裁剪与预期用途无关的能力
  - ✓ 对外通讯能力;
  - ✓ 文件层的存取控制能力
  - ✓ 删除无关的用户账号;
  - ✓ 关闭无关的共享资源
  - ✓ 关闭无关的通讯端口;
  - ✓ 关闭无关的服务，如:Internet FTP IIS 等服务
  - ✓ 关闭/删除无关的应用软件;
  - ✓ 确保器械不能被不受控的移动介质启动
  - ✓ 确保不能在器械上加装未经授权的软硬件

9.数据去标识化与匿名化(DIDT-HEALTH DATADE-IDENTIFICATION):产品直接去除、匿名化数据所含个人信息的能力。

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。

■ 健康数据身份信息去除能力

- ➢ 医疗器械可以内置隐私数据去标识化的能力
  - ✓ 确保当数据作为非医疗用途使用时数据主体身份不被识别。

10.数据完整性与真实性(IGAU-(HEALTH DATAINTEGRITY AND AUTHENTICITY -IGAU):产品确保数据未以非授权方式更改且来自创建者或提供者的能力。

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。

确保数据纯正的能力器械有能力对存储数据进行错误检查，错误纠正。

11.数据备份与灾难恢复(DTBK-DATABACKUP AND DISASTER RECOVERY)产品的数据、硬件或软件受到损坏或破坏后恢复的能力。

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)

■ 数据遭到破坏后的恢复能力

- 医疗器械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。

12.数据存储保密性与完整性(STCF):产品确保未授权访问不会损坏存储媒介所存数据保密性和完整性的能力。

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。

■ 器械在被入侵的情况下，仍然保持数据完整性与保密性的能力

- 器械对数据进行加密处理
- 注意符合国家密码法规

——密码法(2020 年 1 月 1 日起施行)

第二十七条 法律行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营害应当使用商用密码进行保护，自行或者委托商用密码检测机构开展商用密码应用安全性评估。

一商用密码管理条例 (2020 年 08 月 20 日修订草案征求意见稿)

- ✓ 本条例所称商用密码，是指采用特定变换方法对不属于国家秘密的信息等进行加密保护、安全认证的技术、产品和服务。
- ✓ 国家鼓励公民，法人和其他组织依法使用商用密码保护网络与信息安全，鼓励使用经检测认证合格的商用密码。

13.数据传输保密性 (TXCF):产品确保数据传输保密性的能力。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。

- ■ 确保数据传输保密性的能力
- ➢ 尽可能使用点对点的专线来传输隐私数据
  - ✓ 一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。
- ➢ 在通过网络或者移动介质进行传输前，对隐私数据进行加密一同样需要符合国家密码法规
- ➢ 隐私数据的接收方，可仅限于固定清单所列的范围。

14.数据传输完整性(TXIG):产品确保数据传输完整性的能力。

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。

- ■ 使用数据传输的完整性
- ➢ 使用防止数据被篡改的机制
- ✓ 查杀恶意软件
- ✓ 数据校验

15 网络安全补丁升级(CSUP-CYBER SECURITY PRODUCT UPGRADES):授权用户安装/升级产品网络安全补丁的能力。

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。

■ 产品网络安全升级的能力

➢ 当相关操作系统或医疗器械发布了网络安全补丁时，许可用户自行安装相应补丁。

✓ 制造商可能限制用户自行安装升级补丁

✓ 部分补丁可以远程安装。

16.现成软件清单(SBOM):产品为用户提供全部现成软件清单的能力

■ 产品为用户提供全部现成软件清单的能力。

告知并支持运营商医疗设备中包含的商业、开源或现成软件组件的网络安全

用户需求:

➢ 告知并支持运营商.医疗设备中包含的商业、开源或现成软件组件的网络安全 SBOM 通过列出每个软件组件的名称、来源、版本和构建来创建必要的透明度

➢ SBOM 使设备运营商(包括患者和医疗保健提供商)能够有效管理其资产和相关风险，了解已识别的漏洞对设备(和连接的系统)的潜在影响，并部署对策，以维护设备的安全性和基本性能。

➢ 设备操作员可以使用 SBOM 与设备制造商协作，识别可能存在漏洞的软件，更新需求，并执行适当的安全风险管理。SBOM 还通过向潜在买家提供应用程序中使用的组件的可见性，并确定潜在的安全风险，从而帮助他们做出购买决策.

➢ 制造商应该在部署 SBOM 时使用的格式、语法和标记方面利用行业最佳实践由于 SBOM 揭示了有关医疗设备的敏感信息，因此鼓励通过可信的通信渠道分发。

制造商将确定 SBOMs 与操作员通信的可信方式，这是公认的

17.现成软件维护((THIRD-PARTY COMPONENTSIN PRODUCT LIFECYCLEROADMAPS-RDMP RDMP):产品在全生命周期中对现成软件提供网络安全维护的能力

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

- 列明现成软件(操作软件、支持软件、应用软件)
  - 保证信息可得
  - 软件安全升级可以完成

操作系统软件: Windows、 /OS

支持软件:介于操作系统软件和应用软件之间，为了解决当前操作系统下应用软件的使用性和兼容性。是一类软件的泛称。

应用软件:多媒体处理软件、internet 工具软件办公软件

18.网络安全使用指导(SGUD):产品为用户提供网络安全使用指导的能力为系统的操作者和管理员提供安全指南。

- 为操作者、管理员、销售员，维护人员提供网络安全指导
  - 说明书包含
    - ✓ 网络安全相关特性
    - ✓ 彻底清除设备，介质中敏感信息的指导说明

19.网络安全特征配置(CNFS-CONFIGURATION OF SECURITY FEATURES):产品根据用户需求配置网络安全特征的能力。

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。

- 网络安全特性可被灵活配置的能力
  - 医疗器械的拥有者、操作者能重新配置产品的网络安全能力
    - ✓ 必要时制造商可对此项能力予以限制

20.紧急访问(EMRG-EMERGENCYACCESS):产品在预期紧急情况下允许用户访问和使用的能力。

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。

- 器械应对紧急使用能力
  - 必要时器械可以被紧急使用

在紧急医疗环境下，提高可得性而损失其他方面网络安全特征。

21.远程访问与控制(RMOT):产品确保用户远程访问与控制 (含远程维护与升级)的网络安全的能力。

远程访问和控制更新软件时，医疗器械能在访问和控制的过程中保证保密性、可得性、完整性的能力

- ■ 远程访问与控制的网络安全
  - ➢ 通过制造商提供的安全授权远程服务和支持平台进行更新。
  - ➢ 用户根据制造商提供的说明确保远程连接。
  - ➢ 一些家用设备，特别是那些被归类为 Samd(独立软件)的设备，提供远程更新或用户管理的补丁方法。

远程更新需要最少的用户交互，但通常需要患者根据医疗保健提供商建立的流程同意。

22 恶意软件探测与防护(MLDP-MALWARE DETECTION/PROTECTION - MLDP):产品有效探测、阻止恶意软件的能力。

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。

- ■ 医疗器械可以配备反恶意软件
  - ➢ 可由用户自己配置或重新配置反恶意软件
  - ➢ 探测到恶意软件时，可通过用户界面予以通知
  - ➢ 探测到恶意软件时，可由经授权的一方进行修复
- ■ 有制造商安装的反恶意软件，其病毒特征库需要更新时
  - ➢ 可由医疗器械的拥有者、操作者来完成。