ICS 点击此处添加 ICS 号
CCS 点击此处添加 CCS 号

YY

中 华 人 民 共 和 国 医 药 行 业 标 准

YY/T XXXXX—XXXX

医用超声影像软件通用要求

General requirements for medical ultrasound imaging software

(点击此处添加与国际标准一致性程度的标识)

（工作组讨论稿）

（本草案完成时间：20240920）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

国家药品监督管理局　　发 布

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医用超声设备分技术委员会（SAC/TC10/SC2）归口。

本文件起草单位：湖北省医疗器械质量监督检验研究院等。

本文件主要起草人：胡艺等。

医用超声影像软件通用要求

1 范围

本文件规定了医用超声影像软件的通用要求和测试方法。

本文件适用于医用超声影像软件含独立软件和软件组件，如超声影像处理软件、超声影像分析软件、超声影像管理软件、超声影像工作站软件等。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069 信息安全技术术语

GB/T 25000.51 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

GB/T 25000.10 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

GB/T 20984 信息安全技术 信息安全风险评估方法

YY/T 0767 超声彩色血流成像系统

YY/T 1419 超声准静态应变弹性性能试验方法

YY/T 1279 三维超声成像性能试验方法

GB 10152 B型超声诊断设备

3 术语和定义

下列术语和定义适用于本文件。

3.1

响应时间 Response time

指从用户发起一个请求开始到服务器完成对请求的处理并返回处理结果所经历的时间。

3.2

容量 Capacity

指产品或系统参数的最大限量满足需求的程度。

3.3

资源利用率 Resource utilization rate

指产品或系统执行其功能时，所使用资源数量和类型满足需求的程度。

3.4

漏洞 Vulnerability

软件或硬件具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统。

3.5

风险评估 Risk assessment

风险识别、风险分析和风险评价的整个过程。

4 要求

4.1 随附文件

随软件所带的文件，其内容包含了为责任方或操作者提供的信息。

软件的随附文件应包含下列信息：

a） 其自身的唯一识别信息（含软件名称、型号、版本号信息说明）；
b） 超声影像软件预期使用者应具备的知识背景；
c） 超声影像软件说明书文件；
d） 超声影像软件快速操作手册；
e） 如果随附文件分若干部分提供，至少应有一个部分包含对其他所有部分的索引；
f） 软件支持的语言；
g） 品特殊功能说明；
h） 超声影像软件验证中涉及到的验证程序（如自动化脚本文件、DICOM 服务器等）、测试软件等文件及说明；
i） 如有可调用接口，用户可调用的接口和相关的被调用软件；
j） 软件组件的选项和版本。

判定方法：通过检查随附文件、软件测试来检验其是否符合要求。

4.2 软件功能要求

4.2.1 基本功能

4.2.1.1 信息管理功能

具有内置超声图文工作站，应满足如下功能要求：

a） 对于初诊患者，可以以下方式进行检查：
   1） 录入患者相关信息；
   2） 通过本机或者 DICOM 服务器获取存档患者信息；
   3） 需支持在未输入患者信息下，直接执行检查操作。
b） 通过病人 ID 对患者信息进行管理，对图像数据及文件报告进行保存。
c） 对病人进行检查的需支持以下几种方式：新建病人、新建检查、暂停检查、激活检查、继续检查、结束检查、取消检查。
d） 应支持病人信息的存储与修改。宜支持基于检查的数据管理功能，一个病人可以关联一个或多个检查。应支持检查列表显示，可以对每一个检查储存的图像进行预览。应提供数据的搜索功能，用户可以通过关键字搜索本机保存的检查数据。可以对检查数据进行删除、备份与恢复。

判定方法：对照说明书，操作机器是否符合 4.2.1.1 描述要求。

4.2.1.2 联网功能

如适用，应在软件标识联网质量，宜有明显标识对不符合的网络环境进行提示，有线网应该有连接标识符及连接状态显示，无线网应该有信号强度条。网络连接无法满足软件使用基本要求时，应有提示。无线网络应采用加密方式，该加密状态可被客户查询（提示可能会影响客户体验，不建议提示，建议改为可查询加密状态）。无线连接宜显示信号强度 如图形、-dBm数值及当前传输速度Mbps。

判定方法：有线网络通过插拔，查看其符号状态显示是否正确；构建不同强度的无线网络，联网质量无法满足要求时应有4.2.1.2相关的状态提示。

4.2.1.3 注释及体位图功能

支持文字注释、箭头注释、注释描迹。支持添加体位图，可以修改体位图上的探头指示。文本注释需要支持注释词库，用户可以根据不同检查部位选择不同的注释词。用户可以对已添加到图像上的注释词进行编辑或删除。用户也可以通过键盘输入注释词。箭头注释支持箭头方向的调节。文本和箭头注释需要支持颜色与字体大小设置。箭头注释还需要支持不同的箭头样式设置。为了方便用户选择使用体位图，需要提供体标的分类与管理功能。用户可以导入自定义的图片当成体位图使用。

判定方法：在B、C、D、M模式下，可以在超声图像界面上，添加修改注释，注释清晰可见，不会出现错误字符及乱码，可以在超声图像添加体位图，体位图清晰可见，可满足4.2.1.3的功能要求。

4.2.1.4 模式选择功能

软件应具备模式选择功能。成像模式满足基本的B型、C型、D型、M型。

判定方法：实时状态下，进行显示模式切换操作，对应模式按键正常响应，键灯提示正确，可以实现B，C，D，M成像模式的切换。

4.2.2 测量功能

使用国际单位制，设备上参数的数值指示，应采用符合ISO 80000-1的SI单位。应支持不同图像类型下的基础测量功能。如B图像下，应支持距离、面积、角度类测量，且支持不同测量方法；M图像下支持时间、距离、斜率类测量；PW和CW图像下支持速度、时间、速度时间积分。

基于上述基础测量功能，各图像类型下应该支持一系列衍生出来的计算功能，如B图像下，支持体积、长度比、面积比等测量；PW和CW图像下，支持速度时间积分、速度比等。

应支持各应用下的专用测量，具体测量包括常规测量项及各应用区域下的专用测量项。如腹部测量、心脏测量、产科测量、妇科测量、泌尿测量、小器官测量、血管测量、矫形外科测量等。

自动测量功能。如适用，应支持自动识别后的手动修改功能。如产科自动测量功能、IMT自动测量功能。

上述测量数据应支持在系统中展示，并支持发送到外部系统。如支持在报告中展示测量数据，并使用DICOM发送到PACS等外部介质。

判定方法：依据随附文件应用分册说明书中测量单位，检查软件是否有这些单位显示。

4.2.3 软件测量包

应明确软件测量包的类型及含义，包括常规测量软件包、腹部应用软件包、产科应用软件包、妇科应用软件包、心脏应用软件包、泌尿科应用软件包、小器官应用软件包、矫形外科应用软件包、血管应用软件包及其他软件包。软件上应有相应的含义描述。

判定方法：查说明书描述，查看对应检查模式软件界面的测量包。

4.2.4 图像显示

适用时，应明确显示如下指标：当前图像分辨率，探测深度，模式。

判定方法：查看主界面参数显示，应满足4.2.3描述。

4.2.5 图像文件读取功能

支持动态和静态图像文件导出和读取。应明确所支持的图像格式（如：frm、cin等），私有格式应予以注明。支持的报告格式为PDF，能正常读取。

判定方法：工作站查看对应图像的文件格式，应满足4.2.3.1描述。

4.2.6 图像处理功能

4.2.6.1 B型成像

B图像基本参数的可视可调，涉及超声设备通用参数，不含特异性参数。（如：频率、增益、动态范围、灰阶、伪彩、图像深度、扫描范围、焦点、空间复合、扩展成像、图像增强等）

判定方法：对照说明书，操作设备可以满足4.2.4.1描述的各项参数调节。

——可视：调节参数，主界面图像对应调节变化。

——可调：调节挡位或进度条可调节。

4.2.6.2 C型成像

C图像基本参数的可视可调，涉及超声设备通用参数，不含特异性参数 （如：频率、增益、壁滤波、余辉、基线、量程、彩色灵敏度、彩色图谱、支持线阵探头彩色取样框偏转、支持二维彩色双实时、BC同宽等）

判定方法：对照说明书，操作设备可以满足4.2.4.2描述的各项参数调节。

——可视：调节参数，主界面图像对应调节变化。

——可调：调节挡位或进度条可调节。

4.2.6.3 M型成像

M图像基本参数的可视可调，涉及超声设备通用参数，不含特异性参数（如：增益、扫描速度、灰阶、伪彩等）

判定方法：对照说明书，操作设备可以满足4.2.4.3描述的各项参数调节。

——可视：调节参数，主界面图像对应调节变化。

——可调：调节挡位或进度条可调节。

4.2.6.4 D型成像

图像基本参数的可视可调，涉及超声设备通用参数，不含特异性参数。（如：频率、取样容积深度、取样容积、取样线位置、壁滤波、量程、扫描速度、翻转成像、基线、校正角度、取样线偏转角度、多同步、伪彩、灰阶、动态范围等。）

判定方法：对照说明书，操作设备可以满足4.2.4.4描述的各项参数调节。

——可视：调节参数，主界面图像对应调节变化。

——可调：调节挡位或进度条可调节。

4.2.6.5 特殊成像

支持全景成像、3D/4D成像、组织多普勒成像、弹性成像。

判定方法：对照说明书，操作设备，可进入4.2.4.5对应的特殊成像模式。

4.2.7 影像传输

4.2.7.1 静态图像传输

导出时,用户可以选择是否导出超声报告。导出的数据需要提供隐藏敏感信息的选项。宜支持DICOM、HL7网络传输及网络存储。

至少支持一种技术的网络传输功能，注明产品正常使用所需的最低传输速率，传输协议。

网络传输技术可以是有线网、Wi-Fi。

判定方法：搭建随附文件描述的网络环境，验证4.2.5.1。图像传输正常，传输后图像和设备图像保持一致。

4.2.7.2 动态视频传输

需要支持发送到多种目的地，比如：U盘，光盘、手机等。需要支持多种视频格式，比如：AVI、MP4等。导出的数据需要提供“隐藏病人信息”的选项。

判定方法：对照随附文件进行操作，检查是否符合4.2.5.2。注：文件格式的判定不能仅以文件后缀名为依据，宜采用读取文件头文件声明等方式。

4.2.8 影像融合

宜支持以下软件功能：

a) CT/MR 的三维图像数据（DICOM 格式）解析导入超声成像系统；

b) CT/MR 数据中病灶或其他区域的手动/自动标注功能；

c) 超声图像与 CT/MR 图像之间的手动/自动配准功能；

d) 超声图像、CT/MR 图像、肿瘤标记的不同透明度融合叠加实时显示。

判定方法：对照说明书，操作设备，观察操作是否生效。

4.2.9 控制功能

4.2.9.1 灵敏度控制

超声仪器灵敏度与图像清晰度取决于相关功能键的实时调节,需要对设备调节的灵敏度做相应的规范。以超声仪器参数能实时调节为标准。主要指标如：增益（总增益、TGC）、声输出功率、帧率、动态范围、选择检查模式等。应满足相应时间满足临床需要，无明显的迟钝感。同时满足随附文件对相应时间的要求。

判定方法：进行4.2.7.1主要指标的操作，利用合适的工具测试响应时间，图像响应时间应满足4.2.7.1时间要求。响应时间可以进行合成、转换等计算。响应时间在1000ms以下的指标不应用秒表测量。

注：合适的测量工具可以是性能效率测试软件、秒表、高速照相机、编写针对软件的专门脚本等。

4.2.9.2 扫描方式

如适用，软件应明确标注各种扫描方式。满足电子凸阵扫描、电子线阵扫描、电子相控阵扫描、机械三维扫描。

判定方法：检查随附文件探头相关说明，必要时检查软件的设计开发文档。

4.2.10 远程功能

4.2.10.1 远程画面传输

支持实时超声画面同步远程传输，远端可对实时画面做调整切换；宜支持语音、视频同步传输功能，具备超声远程会诊、远程质控、直播教学等功能模块。

判定方法：通过远程网络连接启动系统，远端与超声设备端建立音视频业务连接，检查随附文件，进行软件测试以检测其是否符合要求。

4.2.10.2 远程调节参数

远程调节参数，远端能通过网络显示超声设备系统界面并对参数进行实时调节，包括不限于成像模式切换、测量、放大/缩小、冻结、解冻、添加注释等。

判定方法：通过检查随附文件及必要时进行软件测试来检测其是否符合要求。

4.2.10.3 数据去标识化

系统应具备数据去标识化功能，应使用数据加密技术对敏感数据进行保护。

判定方法：通过检查随附文件及必要时进行软件测试来检测其是否符合要求。

4.2.10.4 远程性能

远程性能：支持标准流媒体的输出，应满足以下要求：网络时延小于200ms，丢包率不大于5%，抖动小于20ms，音视频同步性小于50ms；

判定方法：通过远程网络连接启动系统，远端与超声设备端建立音视频业务连接，使用网络测试仪和音视频流畅度测试设备，测试网络性能及评估音视频同步性能；

4.3 性能效率

4.3.1 响应时间

4.3.1.1 成像时间

如适用，切换模式后成像时间应满足相应时间满足临床需要，无明显的迟钝感。同时满足随附文件对相应时间的要求。（B、C、D基础模式切换，参数应为缺省值）

判定方法：切换B、C、D模式基础模式，从切换到图像响应时间应满足4.3.1.1要求。

4.3.1.2 延迟

出图延时应满足相应时间满足临床需要，无明显的迟钝感。同时满足随附文件对相应时间的要求。（B、C、D基础模式切换，参数应为缺省值）

判定方法：切换B、C、D模式基础模式，从切换到图像响应时间应满足4.3.1.2要求。

4.3.1.3 分析时间

定量分析及AI计算应满足相应时间满足临床需要，无明显的迟钝感。同时满足随附文件对相应时间的要求。应规定最大时长，超过最大时长，软件应给出提示。

判定方法:按照随附文件进行定量分析及AI计算操作,从开始分析计算到出计算结果应满足4.3.1.3要求。

4.3.1.4 图像重建时间

3D图像重建时间（缺省值）应满足相应时间满足临床需要，无明显的迟钝感。同时满足随附文件对相应时间的要求。重建时间为采集结束到3D出图的时长。

判定方法：按照随附文件3D操作，从采集结束到出图应满足4.3.1.4要求。

4.3.2 容量

软件应注明在典型运行环境下（CPU、内存、硬盘、网络带宽）支持的最大并发数或者最大业务量。

判定方法：在随附文件规定的运行环境下，进行最大容量值测试，软件可以持续正常运行。事务的成功率可在随附文件进行规定，不得低于90%，未在文档规定的，按照100%的要求进行测试。测试时应当对随附文件描述的容量数量进行100%、120%测试（冗余测试），两者均需通过，测试次数不得低于3次，连续3次测试结果均需通过，按照文档要求取最大值、平均值。

4.3.3 资源利用率

在4.3.1、4.3.2的条件下对资源的使用要求，CPU使用率应小于90%，内存使用率应小于90%。

判定方法：按照4.3.1、4.3.2的场景运行软件，满足4.3.3要求。

4.3.4 图像质量

应满足厂家提供的该产品技术要求中的性能指标。需参考满足且不低于YY 0767、GB 10152、YY/T 1279、YY/T 1419标准要求。

判定方法：查阅随附文件，产品需求规格说明书等相关文档。

4.4 兼容性

4.4.1 硬件环境

软件应该在文档描述的硬件环境正常运行。通用计算平台包括处理器、内存、硬盘、外设。专用计算平台应当包括平台型号等可以定位到平台稳定配置的信息。如USB接口、打印机远程控制接口、以太网接口、DC电源接口、探头接口、HDMI接口、S-Video接口、脚踏开关、扫描枪等。

判定方法：选择4.4.1所提到的配件，按照随附文件说明书，进行功能连接验证，能正常连接，软件操作配件能正常响应。

4.4.2 操作系统和支持软件

软件应当在文档描述的操作系统和支持软件下正常运行，如操作系统、数据库、三方组件、其他支持软件的名称、版本。

判定方法：随附文件满足4.4.2需求条件下，不会出现系统的 CPU、进程等系统资源占用异常，或者造成其他软件运行错误、系统出错、软件用户界面显示不友好等问题。

4.4.3 互操作性

满足多个软件版本病患数据向下兼容。新版本能查看旧版本上保存的病患数据。

判定方法：提供新旧两个版本，按照说明书进行互操作性测试。满足4.4.3要求。软件应能提供与其他医疗或非医疗产品、系统或设备的数据交换功能，如数据表格、检查报告、医学影像数据的导入或导出功能；宜采用通用协议并明示支持的协议名称、版本。如TLS、DICOM、HL7、TCP/IP等。

4.5 易用性

4.5.1 图标、菜单

软件适用的图标、菜单名称应为医用超声通用、共识、不易造成歧义的名称。软件所用到的对应术语、缩略语或自定义名称应当在软件或用户手册上进行相应说明。

判定方法：检查随附文件和机器，满足4.5.1要求。

4.5.2 消息、提示

软件的消息或提示应当准确、恰当。

判定方法：消息或提示信息模拟，使用弹窗、气泡或其他形式，文字描述提示无歧义，声音提示清晰。

4.5.3 提醒、二次确认

有严重后果或不可撤销的操作应进行提醒和二次确认，应当进行相应的弹窗或声音提醒。

判定方法：错误信息模拟，有相应的错误提示，文字错误提示无歧义，声音提示清晰。文字提示和声音应和4.5.2有等级区分。

4.5.4 影响界面美观与用户操作的情形

用户界面不应出现乱码、不清晰的文字或图片等影响界面美观与用户操作的情形。

判定方法：检查随附文件和机器，满足4.5.4要求。

4.6 可靠性

4.6.1 软件连续工作时间

主要运行场景应满足B、C、D、M模式切换、主要参数调节、应用功能设置等。在产品声明的典型功能场景下持续运行不低于12小时（或在压力场景完成等效业务量），不应该出现死机、软件异常等不可用的问题。随附文件中宜描述平均失效时间间隔（MTBF）、系统可用性（在计划的系统运行时间中，系统实际可用时间的比例是多少）指标，软件失效的具体判定方法。

判定方法：根据随附文件描述编写脚本，设置相应的业务强度持续运行，满足4.6.2要求。脚本测试运行时间不得低于2小时。

4.6.2 资源不足的警告

系统资源不足或接近、超出极限时应发出警告，并有防止系统崩溃的处理措施。断网、存储损坏时发出警告。随附文件宜规定平均故障通告时间指标、故障通告方式。

判定方法：提供模拟测试用例脚本，模拟极限环境，达到4.6.3描述情况，应有相应的错误提示，文字错误提示无歧义，声音提示清晰。

4.6.3 限制范围内操作

用户在文档陈述的限制范围内对产品进行操作时，不应该造成数据的丢失。输入违反句法条件的信息时，产品给出提示。并对违规操作的有相应的处理措施：比如提示、警告等。

判定方法：检查随附文件和机器，满足4.6.3要求。

4.6.4 中断后的恢复

系统发生中断，如死机、运行速度过慢、计算精度不够、输出不符合要求时应具备一定的恢复能力，且已经保存的数据不应丢失；文档中应对中断的处理方式进行陈述，如重启软件、重启服务器、恢复出厂设置或联系供应商处理。随附文件应规定平均恢复时间（软件从失效中恢复需要的时间）指标。

判定方法：检查随附文件和机器，模拟系统中断情形，满足4.6.4要求。

4.7 可移植性

4.7.1 配置与环境

文档应说明软件投入使用应能适应的不同配置与环境，并对其硬件适应性（如主机硬件配置、屏幕分辨率、网络环境等）、软件适应性（如浏览器、操作系统、数据库、中间件等）进行说明。

判定方法：检查随附文件和机器，满足4.7.1要求。

4.7.2 软件

文档应说明如何提供软件安装、卸载、更新服务，如允许用户自行操作，应提供相应的文档。

判定方法：检查随附文件和机器，满足4.7.2要求。

4.8 维护性

4.8.1 系统维护

软件应具备预置数据的导入、导出、恢复出厂设置能力。系统维护含系统升级、系统权限、系统信息显示等。软件宜具备系统预置，探头/检查预置，注释预置，测量预置，DICOM预置功能。

判定方法：

a) 用移动存储介质（U盘，硬盘等）对预置数据进行导入、导出互相迁移操作。
b) 参随附文件，恢复出厂设置，参数恢复出厂值
c) 厂家提供升级文件，对设备进行升级操作，升级完成后查看系统信息显示，版本与所提供的升级文件对应；

4.8.2 易分析性

软件应具备运行日志，出现异常或失效时应记录关键信息；软件宜具备审计日志功能，能够追溯用户的关键操作。

判定方法：操作设备，模拟正常、异常、失效情景，查看是否具备运行日志(日志可以通过软件查看，也可以单独存储)，日志是否记录设备关键操作的名称、时间等信息，软件异常或失效时时日志能否记录事件。审计日志应具备防篡改和保密性功能，审计权限应与管理员权限、用户权限分离。

4.9 网络安全

4.9.1 自动注销、自动锁定能力

如适用，应说明软件自动注销或自动锁定条件，解锁条件。

判定方法：对照随附文件，检查在给定时间内、给定时间后系统是否自动注销或锁定。

4.9.2 审核能力

如适用，软件应具备审核软件活动的功能。审核要素包括用户名、活动时间、活动内容。审核数据应当确保保密性和完整性，即非授权无法查看，无法修改。应确定审核数据的保存最短时间。例如日志审计功能，记录系统事件、网络事件、应用事件。

判定方法：对照随附文件，检查系统是否具备日志记录功能，检查日志记录是否可以修改和删除，日志记录内容是否有事件描述、发生时间、操作账号等要素，满足4.9.2的要求。

4.9.3 授权能力

如适用，软件应当给有明确的权限划分。宜遵循最小权限原则。管理、审核、业务权限宜分离。重要权限的配置宜采用两种及以上认证方式。

判定方法：对照随附文件操作系统，检查权限划分的正确性，验证是否满足4.9.3的要求。注：按照最小权限原则，管理员、审核员角色一般不应具备系统业务操作功能。

4.9.4 节点鉴别能力

如适用，软件应鉴别不同节点信息，鉴别的技术方法不限于IP、MAC、数字证书和数字签名等。即软件能够区分通信的不同节点，且有防伪造通信身份的功能。

判定方法：对照随附文件操作系统，查看不同节点，验证是否满足4.9.4的要求。

4.9.5 人员鉴别能力

如适用，软件应当支持建立不同用户，用户有唯一识别身份，该身份不可更改，且可被软件识别。软件不应显示不可区分的身份，如软件内部采用不同ID记录不同身份，但显示为同样的用户身份信息。软件宜对用户密码强度进行要求，在用户首次登录或一定周期后提示用户修改密码，且不能为初始密码以及当前使用的密码。重要角色登录软件宜采用两种及以上认证方式，如本地、密码、动态、ldap、mldap、生物特征识别、Ukey等。

判定方法：对照随附文件操作系统，新建重名、重复ID用户，验证是否满足4.9.5的要求。采用密码+验证码、数据签名等多因素认证的，应按照资料进行操作验证。采用动态密码的，应当至少测试3次，检查密码是否为动态。

4.9.6 连通性能力

如适用，应采用确保安全联网的协议和连接方式。如点对点有线连接（中间无其他节点或网络交换设备，且连接设备在同一区域），可不采用加密传输。如非点对点有线连接（多点连接，连接对象之间经过交换机等网络设备）的宜采用加密协议。无线连接应采用加密认证协议进行无线连接。连接质量应当保证软件使用的最低要求。

判定方法：对照随附文件操作系统，确保节点之间网络可达。采用加密的，应观察加密技术。验证是否满足4.9.6的要求。

4.9.7 物理防护能力

如适用，应采用物理手段确保数据完整、可控，必须使用钥匙等工具才能接触存储部件。这些手段包括增加物理隔离设施如带门禁的机房、机柜等，USB、网络接口、存储部件物理隔离措施等，特殊环境的电子频闭设施等。

判定方法：对照随附文件观察，设备是否采用物理防护手段阻止非授权人员接触物理存储部件，验证是否满足4.9.7的要求。

4.9.8 系统加固能力

如适用，应有相应的固化措施对网络攻击和恶意程序进行抵御，尽量减小受攻击面。如关闭不必要的系统端口、账号、服务，启用防火墙、防病毒软件或功能，采用ukey启动软件，对软件升级包进行哈希值、校验码进行校验确保为原厂发布，限制安装软硬件等。

判定方法：对照随附文件操作软件，验证是否满足4.9.8的要求。防火墙可以是物理防火墙也可以是防火墙软件，端口检查可以利用本机系统软件也可以通过专业端口扫描工具，防病毒软件应当为专业软件，且病毒库升级到最新版本。

4.9.9 数据去标识化与匿名化能力

如适用，产品应当能够去除、隐匿化数据包含的个人隐私信息。如产品可以直接对个人隐私信息进行删除或隐匿，该隐匿功能在非授权情况下不能获取明文，且明文信息不可直接批量导出。产品具备数据完全清除功能，该清除不可恢复。个人隐私信息参考 GB/T 37964-2019《信息安全技术个人信息去标识化指南》。

可配置是否隐藏或显示隐私数据， 如姓名， 病人ID, 生日， 性别等。隐私数据的显示， 需要支持匿名化。导出数据（包括图片，日志等）的时候， 需要支持脱敏。

判定方法：对照随附文件操作软件，验证是否满足4.9.9的要求。

4.9.10 数据完整性与真实性保障能力

产品确保非授权方式对数据进行删除、修改的能力。产品需确保数据来源真实可靠。

判定方法：对照随附文件操作软件，验证是否满足4.9.10的要求。

4.9.11 数据备份与灾难恢复能力

产品的数据、硬件或软件受到损坏或破坏后的恢复能力。产品应当说明备份措施（内置备份功能或通过操作系统、工具备份），备份周期或备份数量，以及备份和恢复的操作方式。

判定方法：对照随附文件操作软件，验证是否满足4.9.11的要求。数据备份与灾难恢复能力可以通过软件自身功能实现，也可以通过第三方工具、操作系统实现。

4.9.12 数据存储保密性与完整性保障能力

如适用，产品确保未授权访问不能破坏存储部件所存数据的保密性和完整性。宜采用商用密码对数据进行保护。隐私数据采用非明文存储。重要敏感信息宜采用双因素验证身份的方式访问。非授权用户不可对存储数据进行查看、篡改和删除。如提供RAID等存储策略，对存储数据的MD5值进行校验，存储厂商提供技术措施。存储采用CRC等完整性校验方法。对数据库采用完整性校验措施。重要系统宜采用双机异地备份。

判定方法：对照随附文件操作软件，验证是否满足4.9.12的要求。采用商用密码的需查看商用密码技术资料，也可以直接采用有效的商用密码专业评估结果。采用冗余存储和校验码技术的，应当逐个进行验证。

4.9.13 数据传输保密性保障能力

如适用，产品应具备确保数据传输保密的能力。如采用加密数据链路进行传输，如TLS协议、VPN等。

判定方法：对照随附文件操作软件，验证是否满足4.9.13的要求。采用专业工具获取传输协议，采用抓包的方式验证流量是否采用明文传输。

4.9.14 数据传输完整性保障能力

如适用，数据应具备确保数据传输完整性的能力。软件应能识别数据传输过程中是否受到信道噪声干扰或被篡改，如通可靠传输协议、过数字签名、校验码等技术保证传输完整性。无线传输宜考虑满足产品最低需求的信号强度和干扰因素。

判定方法：对照随附文件操作软件，验证是否满足4.9.14的要求。可以通过搭建噪声干扰环境，利用工具尝试篡改传输数据，观察传输所使用的加密协议等方式验证。以下情形可以认为具备传输完整性保障能力：

a) 采用 https 等具备完整性校验能力的协议；
b) 采用数字证书、数字签名、校验码等技术；
c) 采用 tcp 可靠传输协议进行点对点的连接，中间未产生任何节点的。

4.9.15 网络安全补丁升级能力

如适用，产品应具备授权用户安装或升级网络安全补丁的能力。该升级包括现场安装或远程安装。应说明安全补丁的获取途径和安装方式。需要有定期评估安全漏洞和更新的流程。

判定方法：对照随附文件验证是否满足4.9.15的要求。

4.9.16 现成软件清单

如适用，产品应为用户提供全部现成软件清单。如软件组件标识、软件组件的开发商/制造商、软件组件的主要版本号、该设备包含可用于生成设备上安装的软件组件列表的命令或处理方法、现成软件清单更新程序等。

判定方法：对照随附文件验证是否满足4.9.16的要求。

4.9.17 现成软件维护能力

如适用，产品应在生命周期中提供对现成软件提供网络安全维护能力。生产方应能列出所提供的或所需的操作系统（明确版本号）、第三方软件、软件组件清单。生产方应能提供产品所涉及的第三方软件包括系统软件、数据库软件、报告生成器等。

判定方法：对照随附文件验证是否满足4.9.17的要求。

4.9.18 网络安全使用指导能力

如适用，产品应提供网络安全使用指导能力。对使用者是否提供医疗器械网络安全相关特性的文档，包含提供产品、存储介质的数据去标识化指导、培训。不当使用可能在医疗器械网络安全方面造成不可接受的风险说明，对使用者提供产品说明、可索取的披露资料等。需要提供安全文档。

判定方法：对照随附文件验证是否满足4.9.18的要求。

4.9.19 网络安全特征配置能力

如适用，产品具备根据用户需求配置安全特性的能力。产品的拥有者、操作者能够重新配置产品的网络安全特性。

判定方法：对照随附文件验证是否满足4.9.19的要求。

4.9.20 紧急访问能力

如适用，产品在预期紧急情况下允许用户访问和使用的能力。紧急访问需当前用户登录，以当前用户的身份访问紧急访问功能，系统应记录当前用户的紧急访问信息。产品应当区分并限制不可被紧急访问的敏感信息。

判定方法：对照随附文件操作软件，验证是否满足4.9.20的要求。检查紧急访问是否可以访问预期功能，紧急访问记录是否满足4.9.2，敏感数据是否进行管理。

4.9.21 远程访问与控制能力

如适用，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。产品应说明并验证是否允许远程服务连接以进行设备分析、维修、维修等功能（含远程连接的方式、角色、是否有远程提示等）。

判定方法：对照随附文件验证是否满足4.9.21的要求。

4.9.22 恶意软件探测与防护能力

如适用，产品应具备有效探测、阻止恶意软件的能力。该能力可以通过安装反恶意软件工具实现，工具应具备恶意软件的防御、探测、提示、阻止、清除等功能。应说明反恶意软件特征库和策略的升级方式，软件本身具备恶意软件探测与防护能力的，应予以验证。

a) 非嵌入式产品需要安装杀毒软件；
b) 如果不能安装杀毒软件，需要实现：
    1) 禁用不必要的端口和服务；
    2) U盘里面的程序不能自启动；
    3) 启动操作系统防火墙；
    4) U盘只是读取指定目录和指定格式的文件；
    5) 独占运行，如系统启动以后直接运行 doppler；
    6) 支持使用白名单来限制允许在设备上运行的软件和服务。

判定方法：对照随附文件验证是否满足4.9.22的要求

4.9.23 漏洞评估能力

应对医疗器械网络安全进行系统性审查，识别存在于医疗器械网络中的现有漏洞，确定漏洞的等级和危害程度，以及是否采取相应的措施以提升产品的网络安全性能。

在漏洞评估的过程中，应进行漏洞扫描确认医疗器械及其网络环境中是否存在潜在漏洞，扫描结果应参考 CVSS评分规则和漏洞的CVE/CNVD/CNNVD等编号评估系统安全漏洞严重程度。产品不应有中等及以上且无法修复、预防、提供防止被利用措施的漏洞。

判定方法：使用漏洞评估工具进行漏洞评估，验证产品符合4.9.23的要求。漏洞评估的过程包括：

a) 评估范围分析；
b) 确定漏洞扫描策略；
c) 执行漏洞扫描；
d) 漏洞扫描检测结果评估；
e) 已知剩余漏洞的维护。

注：漏洞扫描应进行登录扫描和非登录扫描。漏洞扫描测试方法参见附录A。

4.9.24 风险评估

如适用，医疗器械产品宜按照GB/T 20984-2022所描述的风险评估流程进行风险评估，如图1所示：

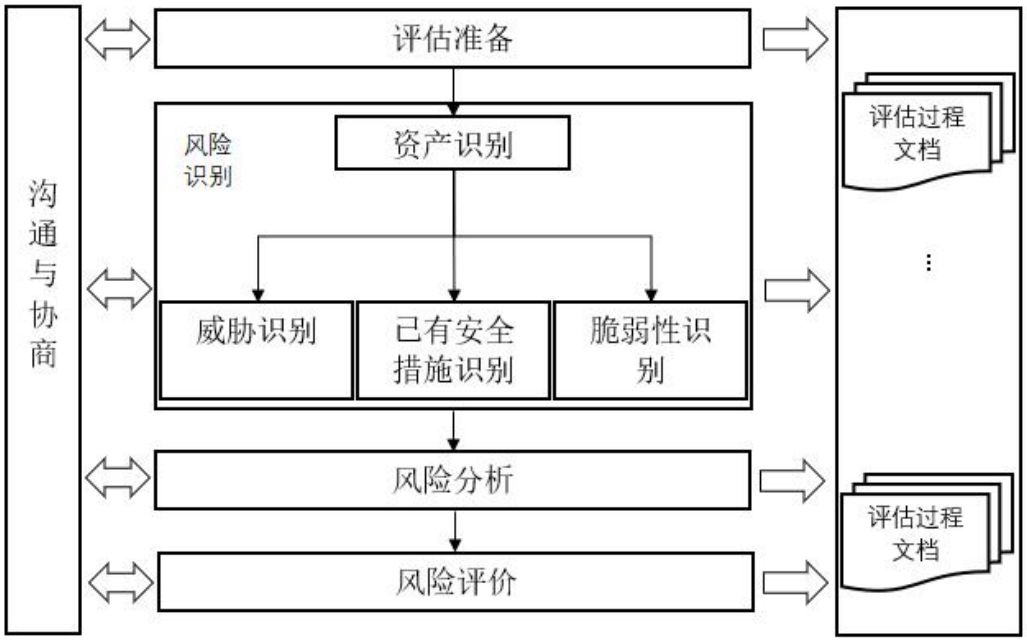

图 1　风险评估流程图

4.9.24.1　资产识别

资产识别是对风险评估的范围进行界定。资产识别范围除了医疗器械产品本身，还应综合考虑必备软硬件、运行环境、业务资产等。资产价值应依据资产的保密性、完整性和可用性赋值，结合业务承载性、业务重要性，进行综合计算，并设定相应的评级方法进行价值等级划分，等级越高表示资产越重要，详见表1。

表 1　资产价值等级表

等级	标识	系统组件和单元资产价值等级描述
1	很低	综合评价等级为很低，安全属性破坏后对业务和系统资产造成很小的影响，甚至忽略不计
2	低	综合评价等级为低，安全属性破坏后对业务和系统资产造成较低的影响
3	中等	综合评价等级为中，安全属性破坏后对业务和系统资产造成中等程度的影响
4	高	综合评价等级为高，安全属性破坏后对业务和系统资产造成比较严重的影响
5	很高	综合评价等级为很高，安全属性破坏后对业务和系统资产造成非常严重的影响

4.9.24.2　威胁识别和已有安全措施识别

威胁识别的内容包括威胁的来源、主体、种类、动机、时机和频率。威胁赋值应基于威胁行为，依据威胁的行为能力和频率，结合威胁发生的时机，进行综合计算，并设定相应的评级方法进行等级划分，等级越高表示威胁利用脆弱性的可能性越大，详见表2。

表 2　威胁赋值表

等级	标识	威胁赋值表
1	很低	根据威胁的行为能力、频率和时机，综合评价等级为很低
2	低	根据威胁的行为能力、频率和时机，综合评价等级为低
3	中等	根据威胁的行为能力、频率和时机，综合评价等级为中等
4	高	根据威胁的行为能力、频率和时机，综合评价等级为高
5	很高	根据威胁的行为能力、频率和时机，综合评价等级为很高

安全措施可以分为预防性安全措施和保护性安全措施两种。预防性安全措施可以降低威胁利用脆弱性导致安全事件发生的可能性，保护性安全措施可以减少安全事件发生后对组织或系统造成的影响。

在识别脆弱性的同时，评估人员应对已采取的安全措施的有效性进行确认。安全措施的确认应评 估其有效性，即是否真正地降低了系统的脆弱性，抵御了威胁。

4.9.24.3 脆弱性识别

对软件及运行环境存在的脆弱性（漏洞）进行识别，详见4.2.9.23要求。如果脆弱性没有对应的威胁，则无需实施控制措施，但应注意并监视他们是否发生变化。如果威胁没有对应的脆弱性，也不会导致风险。控制措施的不合理实施、控制措施故障或控制措施的误用本身也是脆弱性。控制措施因其运行的环境，可能有效或无效。脆弱性赋值时包括两部分，一部分是脆弱性被利用难易程度赋值，详见表3，一部分是影响程度赋值，详见表4。

表 3 脆弱性被利用难易程度赋值表

等级	标识	定义
1	很低	实施了控制措施后，脆弱性基本不可能被利用
2	低	实施了控制措施后，脆弱性难被利用
3	中等	实施了控制措施后，脆弱性被利用难易程度一般
4	高	实施了控制措施后，脆弱性较容易被利用
5	很高	实施了控制措施后，脆弱性仍然很容易被利用

表 4 脆弱性影响程度赋值表

等级	标识	定义
1	很低	如果脆弱性被威胁利用，将对资产造成的损害可以忽略
2	低	如果脆弱性被威胁利用，将对资产造成较小损害
3	中等	如果脆弱性被威胁利用，将对资产造成一般损害
4	高	如果脆弱性被威胁利用，将对资产造成重大损害
5	很高	如果脆弱性被威胁利用，将对资产造成特别重大损害

4.9.24.4 风险分析

根据系统资产识别、威胁识别、脆弱性识别的赋值，采用相乘法计算，确定风险值对应的风险等级。

单项风险值计算公式如下：

$$\mathrm{Rvj} = \sqrt{\sqrt{V \times Di} \times \sqrt{T \times Av}} \quad (1)$$

式中：

Rvj ——单项风险值；

V ——资产的价值等级；

Di ——脆弱性的漏洞程度赋值；

T ——脆弱性对应威胁的赋值（如果脆弱性对应多个威胁则取对应威胁赋值的平均值）；

Av ——脆弱性在已经采用的安全措施的情况下被利用的难易程度赋值。如果风险由多个威胁或者脆弱性分析得出，威胁或脆弱性相关赋值为平均值。

如果风险值很高，不可接受，仍需要采取控制措施进行管理和降低风险。

根据风险值计算公式和影响风险值的各个因素取值范围可以知道，采用相乘法计算风险值的取值范围为 1-25。为实现对风险的控制与管理，参照评估指南对风险值进行等级化处理，将风险等级划分为五级，每个等级代表了相应风险的严重程度，等级越高，风险越高。

4.9.24.5 风险评价

首先计算各个资产对应的总体风险值计算方法为资产对应的所有脆弱性风险值的平均值。

总体风险值计算公式如下：

$$\mathrm{Raj} = \frac{Rv1+Rv2+\cdots+Rvn}{n} \quad (1)$$

式中：

Raj ——总体风险值；

Rvn ——资产n对应的脆弱性风险值；

n ——资产。

综合系统风险值根据资产价值等级对资产风险值进行加权平均计算。

综合系统风险值计算公式如下：

$$Rb = \frac{A1 \times Ra1 + A2 \times Ra2 + \cdots + An \times Ran}{A1 + A2 + \cdots + An} \quad (2)$$

式中：

Rb ——综合系统风险值；

An ——资产的价值等级；

Raj ——各个资产对应的总体风险值，计算方法为资产对应的脆弱性风险值的平均值。

产品综合风险值应当在中级及以下。

判定方法：对产品进行信息安全风险评估，观察其结果是否满足4.9.24的要求。

5 测试要求

5.1 结果判定准则

4.2～4.9均应满足各项描述要求。

5.2 环境

5.2.1 测试所使用的计算设备、网络设备性能不得高于随附文件要求。

5.2.2 测试所使用的操作系统和其他软件如随附文件没有明确具体版本，应为对应的最低版本。

5.2.3 无线网络测试时，除随附文件有特别要求，被测设备与无线发射设备距离不大于 10 米，且中间无遮挡。不高于产品说明要求的 wifi 协议版本（如 wifi5、wifi6），无线连接速率。

5.2.4 测试所使用的安全工具漏洞库应为测试时的最新版本。

附 录 A
（资料性）
漏洞扫描测试方法

A.1 评估范围分析

网络安全漏洞的评估范围不局限于医疗器械软件产品本身，还应考虑运行环境、必备软硬件等。在进行医疗器械网络安全漏洞扫描评估时，应提供产品运行所必需的其他医疗器械软件、医用中间件及医疗器械硬件产品处在正常的配置和运行条件。

A.2 确定漏洞扫描策略

A.2.1 总则

应结合被扫描对象的应用特点及使用环境,恰当地选择扫描工具与方法。制定相应的漏洞扫描策略。

A.2.2 基于网络部署扫描策略

如产品基于网络的部署方式（包括局域网和广域网），漏洞扫描时使用基于网络的扫描方式。基于网络的扫描通过网络探测医疗器械，扫描的范围包括医疗器械产品及其所使用的网络环境。

基于网络的部署方式，通过获取可访问的 IP 地址或域名进行扫描。对于混合部署方式，漏洞扫描工具应分别接入其相应的使用网络中进行扫描。

A.2.3 基于主机扫描策略

如果产品是单机部署，而非基于网络的方式，则在漏洞扫描时使用基于主机的扫描方式。可将漏洞扫描工具与医疗器械产品接入同一局域网内，通过 IP 地址进行扫描。基于主机的扫描针对医疗器械产品自身，主要是对产品内置操作系统和应用程序的漏洞扫描。

对于部分不含有网络连接或远程访问与控制的医疗器械，但存在非网络接口的其他电子接口（如串口、并口、USB 口、视频接口、音频接口等）或通过存储媒介（如光盘、移动硬盘、U 盘）进行数据交换，不对传输协议进行扫描，应对相应电子接口的调用过程进行扫描。

基于主机的漏洞扫描，应根据不同的检测目标，如 Windows、Linux 、Andriod、iOS的区别等，使用恰当的扫描工具，或在扫描工具上进行不同的配置。

A.2.4 嵌入式软件扫描策略

如果产品属于嵌入式软件，软件通过交叉编译，烧录到目标平台，则通过对固件文件或源代码进行检测评估。漏洞扫描方式主要有以下两种：

a) 通过代码审查工具静态分析程序特征；

b) 部署在嵌入式扫描工具中通过自动化脚本进行动态扫描。

A.3 执行漏洞扫描

A.3.1 总则

在执行漏洞扫描前，需要获得被测试方的授权，并按照产品技术要求描述的内容，使被测产品运行在典型使用环境中。

A.3.2 网络部署扫描和主机扫描

应开放所有预期使用的端口，并开放相应的安全策略（如关闭防火墙等），使扫描工具与被测对象之间处于一种无过滤的通信状态，以扫描到完整的目标。

对于基于 B/S（Brower/Server，浏览器/服务器）架构的产品，对服务器端主机进行扫描；

对于基于 C/S（Client/Server，客户机/服务器）架构的产品，应对客户端和服务器端主机分别进行扫描。

漏洞扫描通常分为以下三个阶段：

第一阶段：发现扫描目标

对于基于网络部署的情形，通过将漏洞扫描工具接入产品使用的网络环境中探测到目标主机。

对于基于单机部署的情形，通过将漏洞扫描工具与医疗器械产品直连或内置于医疗器械中，从而探测到扫描目标。

第二阶段：搜寻目标信息

当扫描工具发现目标后进一步搜集目标信息，包括操作系统类型、开放的端口、运行的服务、使用的协议类型等。

对于基于 B/S 架构的产品，扫描的对象还应包括服务器端 Web 应用程序，并且进行扫描过程中登录系统的测试账户应保证能够遍历到系统的所有功能。

第三阶段：扫描测试

根据搜集到的信息，由漏洞扫描工具向搜寻到的目标发送请求信息、返回分析信息，从而最终确定是否存在安全漏洞。

A.3.3 嵌入式软件扫描

基于嵌入式软件的扫描，应使用相应的工具对嵌入式软件固件文件进行扫描分析。

整个分析流程主要分为三个阶段：

第一阶段：识别固件结构体系，提取出待分析的目标程序；

第二阶段：识别固件中存在的成分，如操作系统、第三方库文件、应用程序等；

第三阶段：通过静态分析技术对固件成分进行分析，并与分析工具中内置的漏洞库进行匹配，找出待测软件中存在的漏洞。

对于移动医疗设备，使用移动计算机终端，漏洞评估时对其应用软件的安装包文件进行扫描检测。如果应用软件可以运行在不同的终端环境，如 iOS 系统、Android 系统等，需对不同环境下的安装包文件进行扫描检测。如果移动医疗设备使用通用计算机终端，则采用基于主机或网络部署的方式进行扫描检测。

A.4 漏洞扫描检测结果评估

对医疗器械产品完成扫描检测后，应对该次扫描检测的结果进行描述，记录检测过程中的信息，说明漏洞分布情况，并输出漏洞信息和评估结果。检测结果应包含以下信息：扫描概况、漏洞分布、漏洞详情、被测产品信息、CVSS评分、扫描工具及漏洞库信息等。

A.5 已知剩余漏洞的维护方案

根据扫描后的已知剩余漏洞及其分布情况，产品责任人应针对剩余漏洞的具体信息、漏洞的风险等级、漏洞出现的位置、漏洞修复的难易程度、漏洞修复的紧迫性等方面，并结合风险管理综合分析剩余漏洞对产品安全性方面的影响，确定补偿剩余漏洞的网络安全策略，制定剩余漏洞维护方案。