ICS 11.040.50
CCS C 43

YY

中华人民共和国医药行业标准

YY/T 1861—2023

医学影像存储与传输系统软件专用技术条件

Particular specification of picture archiving and communication system software

2023-01-13 发布　　2024-01-15 实施

国家药品监督管理局　发布

刮涂层 查真伪

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医用X射线设备及用具分技术委员会(SAC/TC 10/SC 1)归口。

本文件起草单位：辽宁省医疗器械检验检测院、国家药品监督管理局医疗器械技术审评中心、中国医学科学院北京协和医院、辽宁省检验检测认证中心、浙江省医疗器械审评中心、中国食品药品检定研究院、上海市医疗器械检验研究院、通用电气医疗系统贸易发展(上海)有限公司、西门子医疗系统有限公司、佳能医疗系统(中国)有限公司、武汉联影医疗科技有限公司、爱克发医疗系统设备(上海)有限公司、富士胶片(中国)投资有限公司。

本文件主要起草人：张龙达、孙智勇、李非、鲍雅晴、孙昊、陈福军、朱文武、李澍、刘重生、秦川、李雅敬、李巍、明星、张锦平、汤稚炜。

医学影像存储与传输系统软件
专用技术条件

1 范围

本文件规定了医学影像存储与传输系统软件的要求和检验方法。

本文件适用于医学影像存储与传输系统软件。

本文件不适用于不使用 DICOM 协议的影像存储与传输系统。

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 18030 信息技术 中文编码字符集

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

3 术语和定义

GB/T 25000.10 界定的以及下列术语和定义适用于本文件。

3.1

医学影像存储与传输系统软件 picture archiving and communication system software

在医学影像获取之后提供存储、传输，还可包括显示、处理功能的软件。

3.2

医学影像云服务(云服务) cloud-based medical imaging service

基于公有云或私有云提供的，用于诊断的医学影像的存储、传输，还可包括显示、处理等服务。

3.3

随附文件 accompanying document

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。

3.4

操作者 operator

操作软件的人。

[来源：GB 9706.1—2020，3.73，有修改]

3.5

用户 user

使用软件并获得收益的组织或个人。

注：用户角色和操作者角色可能被同时赋予或先后赋予相同的个人或组织。

[来源：GB/T 25000.51—2016，4.1.25，有修改]

3.6

责任方　responsible organization

对某软件的使用和维护负有责任的实体。

[来源:GB 9706.1—2020,3.101,有修改]

3.7

提示　prompt

用于请求或指导操作者的响应的,程序所发出的视觉或听觉消息。

[来源:ISO/IEC/IEEE 24765:2017,3.3205,有修改]

3.8

影像视窗　image view port

用于显示影像的最小界面单元。

3.9

标注标识　annotative dimension

叠加在影像上用于标示与位置有关的发现、测量结果、测量基准的图形、文字或符号。

3.10

影像附加信息　attached image information

属于某一影像的患者信息、影像参数信息和其他信息。

3.11

影像合并　image merge

将原本列于多项条目下的影像数据合并到同一条目中。

注:条目的层次可能是患者、检查或序列等。

3.12

可视化　visualization

以不同于其原始状态的形式显示目标影像,从而向操作者展示影像中储存的特定信息的功能。

3.13

渐进式加载　progressive loading

首先显示低分辨率或对比度的影像,再显示完整影像的影像加载方式。

3.14

数据冲突　data conflict

对一项数据作出与已应用的版本不可调和的版本改变。

3.15

事务　transaction

在测试中划分的若干请求的集合,通常代表一个功能点或工作流。

3.16

最大并发事务数　maximum concurrent transaction

事务吞吐量达到最大值时,软件所承受的并发事务数。

3.17

事务吞吐量　transaction throughput capacity

在单位时间内软件能够处理完成的事务量,单位是 TPS[每秒事务数,S 也可替换为 M(分钟)、H(小时)等]。

3.18

影像处理容量　image processing capacity

对于指定的影像处理或影像存储功能,软件能够处理的单次最大数据量。

3.19

事务响应时间　transaction response time

操作者发起一个事务开始，服务器完成对该事务的请求的处理并返回处理结果所经过的时间。

3.20

事务成功率　transaction success rate

正确执行的事务数与全体事务数的比率。

3.21

断言　assertion

指明在程序执行过程中的一个特定位置处，必定存在的程序状态或程序变量必定满足的一系列条件的逻辑表达。

[来源：ISO/IEC/IEEE 24765:2017，3.247，有修改]

3.22

健康数据　health data

与身体或心理健康相关的个人敏感数据。

注：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，健康数据可能会变更为“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法规。

[来源：IEC/TR 80001-2-2:2012，3.7，有修改]

3.23

个人信息　personal information

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

[来源：GB/T 35273—2020，3.1]

3.24

去标识化　de-identification

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

注：去标识化建立在个体基础上，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信息的标识。

[来源：GB/T 35273—2020，3.15]

4　要求和检验方法

4.1　通用要求

4.1.1　软件的随附文件应陈述下列信息：

a)　其自身的唯一识别信息；

b)　软件预期使用者应具备的知识背景；

注：这些知识背景可能包括医学领域的专业与资格、计算机领域的专业与资格和中文以外的其他语言等。

c)　软件是否允许用户进行安装操作；

d)　如果允许用户进行安装，应给出安装规程以及安装所要求的最小磁盘空间；

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)　软件产品的边界；

g)　软件组件的选项和版本；

h） 用户可调用的接口和相关的被调用软件；

i） 软件支持的语言；

j） 术语和缩略语的定义；

k） 软件的载体。

通过检查随附文件及以下方法来检验是否符合要求：

——对于 a)中的要求，唯一识别信息可以是软件的名称、型号及版本号；

——对于 f)中的要求，可以用软件的边界接口和软件包含的功能点共同定义。

4.1.2 软件的执行过程与结果应与随附文件的陈述一致。

通过检查随附文件、软件测试来检验其是否符合要求。

4.2 功能性与易用性

4.2.1 通用要求

软件及其随附文件应符合以下要求：

a） 随附文件应陈述用户能够使用的所有软件功能的执行与结果；

b） 随附文件中陈述的软件功能应是可测的或可验证的；

c） 随附文件应陈述所有客观的使用限制；

注 1：使用限制包括用户使用或管理的数据的长度、数量、句法条件等客观约束。

d） 软件中用于标记的符号，其含义应在随附文件中解释；

e） 除非在与用户交互时提供提示，软件中每一用户交互元素的含义应在随附文件中解释；

注 2：用户交互元素包括按钮、菜单、视窗、快捷键等。

f） 每个软件出错消息应指明如何改正差错或向谁报告差错；

g） 对具有严重后果的功能执行应是可撤销的，或者软件应给出这种后果的明显警告，并且在这种命令执行前要求确认；

h） 随附文件应给出软件与外部实体、软件客户端与服务器的应用层传输协议；

i） 随附文件应给出或索引软件所支持的数据传输与储存规范。

通过检查随附文件、软件测试，必要时检查软件的设计开发、验证与确认文档，及以下方法来检验其是否符合要求：

——随附文件中说明的所有功能和典型工作流中的功能组合，均应经测试用例测试；

——随附文件中说明的每个功能至少应经一个测试用例测试；

——随附文件中说明的所有使用限制均应经测试用例测试。

4.2.2 影像接收与发送

软件的影像接收与发送功能应符合以下要求：

a） 软件应能与符合随附文件中要求的其他实体进行影像接收与发送；

b） 当被请求接收的影像不符合数据传输与储存规范时，软件应拒绝接收影像并通知影像接收行为的发起者，或接收影像并将其与符合规范的影像作出明显区分；

c） 当收到发送影像被拒绝的消息后，软件应提供包含被拒绝的影像、拒绝方信息和时间戳的记录信息；

d） 软件应给出处于影像接收与发送状态的指示；

e） 当软件处于影像接收与发送状态时，会导致接收与发送中断的行为应有需要操作者确认的提示。

通过检查随附文件、软件测试，必要时检查软件的设计开发、验证与确认文档来检验其是否符合

要求。

4.2.3 影像附加信息

软件可支持操作者录入和接口传入(以下简称“录入和传入”)的影像附加信息的输入方式。

对于支持影像附加信息输入的软件:

a) 用于录入影像附加信息的每一个文本框或类似部件,应有输入长度和/或输入规则限制;

b) 除了具有特殊格式或含义的字段外,对于姓名及健康数据文本的录入与显示应支持中文,用于显示的封装字符集应符合 GB 18030 相关要求;

注 1:具有特殊格式或含义的字段,例如:年龄。

c) 应在随附文件中给出影像附加信息的录入和传入限制;

注 2:包括表单中字符的格式、支持的字符集、英文大小写的区分等。

d) 对于不符合录入规则的影像附加信息,应无法录入,或在录入或提交时给出提示,且允许操作者对其再次编辑;

e) 进行会导致录入中的影像附加信息丢失的操作时,应有需要操作者确认的提示;

f) 对于支持由操作者按照某一录入的影像附加信息对影像进行检索的软件,录入功能所支持的字符格式应被检索功能完全覆盖;

g) 提交了影像附加信息的修改后,影像列表及影像视窗中正在显示的相应信息应立即更新或有需要更新的提示。

通过检查随附文件、软件测试,必要时检查软件的设计开发、验证与确认文档,及以下方法来检验其是否符合要求:

——对表单的输入的测试可以采用字符生成器进行录入,但在设计字符生成器时,应有适当的规则来确保生成结果能够遍历每一种支持的格式或长度;如果使用预先准备好的参数表时,同样应对参数表进行上述检查;

——对于 g)中的要求,测试时应考虑修改信息与显示信息位于不同客户端的情形。

4.2.4 影像导入与导出

软件的影像导入与导出功能应符合以下要求:

a) 软件应能按照数据传输与储存规范进行影像导入与导出;

b) 软件应给出影像导入状态的指示;

c) 影像未能正确导入或导出时,软件应给出提示;

d) 软件应对导入影像的格式加以限制,限制的规则与机制应在随附文件中指明;

e) 当导出为有损影像时,界面上应有提示;

f) 随附文件中应给出软件支持的所有可由操作者导出的影像、附加信息和报告及其导出格式。

通过检查随附文件、软件测试,必要时检查软件的设计开发、验证与确认文档,及以下方法来检验其是否符合要求:

——对于 b)中的要求,其形式可以是进度条、状态标记、虚拟指示灯等;

——对于 c)中的要求,测试时应考虑存储空间不足、数据传输中断、超时、校验和错误、目的地存在同名文件或文件夹等情形;

——对于 d)中的要求,测试时应考虑错误的扩展名、空扩展名、伪造的文件头等情形。

4.2.5 影像索引与调阅

软件应支持对内部和/或外部的影像索引与调阅服务。

通过软件测试及必要时检查软件的设计开发、验证与确认文档来检验其是否符合要求。

4.2.6 影像存储与访问

软件的影像存储与访问功能应符合以下要求：

a) 当软件使用压缩方法存储影像时，随附文件中应给出压缩的压缩率、均方误差与相应的图像熵，并通过测试进行验证；

b) 如软件不能支持多个操作者同时对某一影像或附加信息进行编辑，应提供数据锁功能，被设置数据锁的影像应仅能被特定操作者编辑、传输或删除；

c) 受数据锁影响的数据应有标识；

d) 其他操作者试图编辑、传输或删除被设置数据锁的数据时，应有提示；

e) 数据锁应可以由设置数据锁的操作者、管理员或适当时自动解除；

f) 当数据锁不能随着第一个编辑数据的操作者的访问被自动执行时，应有数据冲突检查机制；

g) 随附文件应陈述软件对数据冲突的处理方式，并通过测试加以验证；

h) 数据冲突不应导致数据丢失。

通过检查随附文件、软件测试，必要时检查软件的设计开发、验证与确认文档，及以下方法来检验其是否符合要求：

——对于 a)中的要求：

压缩率(CR)的计算方法见公式(1)：

$$CR = \frac{F}{G} \times 100\% \quad \cdots\cdots(1)$$

式中：

F ——原始影像的字节数(F 应远大于磁盘的分配单元大小)；

G ——将原始影像存储至被测软件后存储该影像所占用的磁盘空间。

原始影像的一维熵(H)的计算方法见公式(2)：

$$H = \sum_{i=0}^{2^k-1} P_i \log P_i \quad \cdots\cdots(2)$$

式中：

P_i ——原始影像中灰度值为 i 的像素所占的比例；

k ——原始影像的存储位深。

均方误差(MSE)的计算方法见公式(3)：

$$MSE = \left\{ \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} [f(x,y) - g(x,y)]^2 \right\} / MN \quad \cdots\cdots(3)$$

式中：

$g(x,y)$——原始影像矩阵($0 \leqslant x \leqslant M-1$，$0 \leqslant y \leqslant N-1$)；

$f(x,y)$——存储至被测软件并读取出的影像矩阵($0 \leqslant x \leqslant M-1$，$0 \leqslant y \leqslant N-1$)；

M ——影像像素列数；

N ——影像像素行数。

使用 10 幅像素矩阵、位深相同的原始影像通过上述方法进行测试并分别计算和记录 CR、H、MSE 的平均值，作为最终的测试结果。

——对于 g)、h)中的要求，测试时应考虑操作者录入信息冲突、影像存储(归档)时冲突、从影像附加信息中自动读取患者信息时冲突等情形。

4.2.7 影像合并

对于支持影像合并功能的软件，应符合以下要求：

a) 应在合并前进行合并规则检查；

b) 对于重复的影像，合并时应分别存储或让操作者选择是否覆盖。

通过软件测试，必要时检查软件的设计开发、验证与确认文档，及以下方法来检验其是否符合要求：

——对于 a)中的要求，当软件通过指定的规则直接阻止合并操作时，或给出提示要求操作者进一步确认时，均视为符合要求；

——对于 b)中的要求，测试时应考虑影像唯一编号(UID)重复，以及其他影像附加信息数据重复、不一致和为空的情形。

4.2.8 影像显示

对于支持预期用于诊断的影像显示的软件，应符合以下要求：

a) 随附文件中应规定支持显示的所有影像模态，以及每个影像模态所支持的可视化功能；

b) 应支持显示影像的平移、翻转功能；

c) 应支持显示影像的缩放功能；

d) 应支持显示影像的窗宽/窗位调节功能；

e) 对于支持多层序列影像显示的软件，应支持在序列内进行影像滚动翻页的功能；

f) 对于支持导入或接收影像图层上的叠加信息的软件，应支持对其进行显示；

注：例如：DICOM GSPS 标记。

g) 对于支持包含预期用于诊断的视图的多显示器布局的软件，应有方法使影像显示在用于诊断的显示器上。

通过检查随附文件、软件测试，必要时检查软件的设计开发、验证与确认文档，及以下方法来检验其是否符合要求：

——影像显示测试所使用的数据应包括标准影像文件、影像显示条件信息以及预期的显示效果；

——应对每一个支持的影像模态进行所有要求的测试。

4.2.9 测量功能

对于软件中给出物理尺寸的手动几何测量功能：

a) 随附文件应给出获得对测量结果进行不确定度评定所需的必要信息，包括对由扫描设备和扫描物产生的输入量的不确定度分量的识别、由软件和运行环境的设置与使用产生的输入量的不确定度分量的评价方法以及合成不确定度的计算方法。

注：对于测量功能的不确定度评定，见附录 A 和 GB/T 27418。

b) 已绘制的测量数值不应受影像缩放、平移、旋转等操作的影响；

c) 影像上的测量标注标识不应随着对影像的平移、翻转、缩放等操作而改变与影像间的相对位置和尺寸关系；

d) 在一个影像视窗中存在多个测量时，应有方法确认数值和测量标注标识的对应关系；

e) 影像中显示的测量标注标识与影像应能区分。

通过检查随附文件、软件测试，必要时检查软件的设计开发、验证与确认文档，及以下方法来检验其是否符合要求：

——应遍历每个测量工具；

——应遍历二维原始影像，以及体数据经可视化功能重建后的二维和三维影像。

4.2.10 数据删除

软件的数据删除功能应符合以下要求：

a) 操作者主动执行数据删除操作，或执行将会导致数据被删除的一系列预置操作时，软件应给出

要求操作者确认的提示并提供取消该操作的功能，或提供撤销删除操作的功能；

b) 具有自动删除功能的软件，应确保自动删除的配置默认关闭，并需要已由操作者配置明确且合理的删除条件后方可执行；

c) 如果软件对已存储(归档)的影像具有手动批量删除或自动删除功能，应能判断存储(归档)到其他存储的请求是否已成功执行。

通过检查随附文件、软件测试，必要时检查软件的设计开发、验证与确认文档，及以下方法来检验其是否符合要求：

——对于 a)中的要求：

- 测试时不包括文本编辑中的删除操作；
- 应考虑遍历所有可被删除的数据类型(例如：用户、角色、患者、检查、序列、影像、报告等)；
- 应考虑遍历所有删除操作的调用形式(例如：按钮、右键菜单、快捷键、手势、触摸屏操作等)。

——对于 b)中的要求：

- 应考虑当用做判定删除条件的参数为空、格式非法或覆盖了所有数据条目的情形；
- 对基于系统时间判定删除条件的机制而言，不合理的条件可以是当前的系统时间与上一次正确启动软件时的时间相比，或者系统时间与某一用做参考的时间来源相比，超过特定的阈值。

注：该设定可以在一定程度上避免由于误操作或主板电池耗尽等原因更改系统时间导致自动删除机制错误触发。

4.2.11 诊断影像误用的防止

软件应能防范可以预见的对诊断影像的误用：

a) 当显示影像窗格中包含多于一个患者的影像，或同一个患者同类型的多个检查时，应显示相应的影像附加信息进行区分；

b) 如软件具有渐进式加载功能，应在影像未达到完整分辨率时给出提示且无法使用需要完整分辨率影像的工具；

c) 当前系统所设置的屏幕分辨率以及界面缩放不能满足软件规定的范围时，应给出提示；

d) 支持将影像以真实尺寸进行显示的软件，在运行环境不满足真实尺寸显示要求时，应给出当前的显示非真实尺寸的提示；

e) 当某一影像显示功能提供给非医疗机构或个人、使用了有损压缩，或预期在非医疗环境下不用于诊断用途显示时，应有提示并在随附文件中说明。

通过检查随附文件、软件测试，必要时检查软件的设计开发、验证与确认文档，及以下方法来检验其是否符合要求：

——对于 e)中的要求，当压缩的均方误差 MSE$\leqslant 1\times10^{-6}$时，可不视为有损压缩。

4.3 性能效率

4.3.1 容量

4.3.1.1 最大并发事务数

随附文件中应给出软件在指定的运行环境下最大并发事务数。

最大并发事务数应与测试工作流、事务吞吐量、事务响应时间、允许的最低事务成功率一并给出，其中事务成功率不应低于 90%。

软件的最大并发事务数、事务吞吐量、事务响应时间、事务成功率及其资源利用性(见 4.3.3)应符合随附文件中的要求。

通过检查随附文件，软件测试，必要时检查软件的设计开发、验证与确认文档，及以下方法来检验是否符合要求。测试工作流应包括：

——被测软件客户端的用户登录、查询、首幅影像加载；

——外部应用实体向被测软件存储(归档)影像；

——外部应用实体向被测软件检索影像列表，并获取影像。

推荐的测试典型影像：512×512 重建矩阵、含有 2 幅影像的 CT 序列。

当存在缓存时，最大并发事务数测试应关闭缓存功能或对查询的信息和读取的影像进行参数化，以确保每个虚拟用户每次请求的信息都是不同的。

在测试过程中，应对事务吞吐量、事务响应时间、事务的成功率以及资源利用性进行监控。

在测试中可不设置集合点。

测试的持续时间应保证成功执行的事务总数大于最大并发事务数的 4 倍，并不低于 5 min。

应使用等于随附文件中规定的最大并发事务数 100%的虚拟用户及 90%的虚拟用户分别进行并发测试，如前者的事务吞吐量小于或等于后者，视为并发测试失败。

应在关键步骤中设计适当的断言以判断结果的正确性，从而计算事务成功率，而非仅通过请求返回的类型(例如：http 请求响应为 200)进行判断。

4.3.1.2 影像处理容量

随附文件中应给出软件在指定的运行环境下的影像处理容量，至少包括支持的最大单一序列影像数和支持的最大总影像数。

通过检查随附文件、软件测试，必要时检查软件的设计开发、验证与确认文档，及以下方法来检验其是否符合要求。

——当处理指定容量的影像时软件崩溃、失去响应视为测试不通过。

4.3.2 时间特性

随附文件中应给出软件在指定的运行环境下的事务响应时间。

随附文件中应给出影响时间特性的内部和外部的变量，以及这些变量在进行测试时的约束条件。

软件的时间特性及其资源利用性(见 4.3.3)应符合随附文件中的要求。

通过检查随附文件、软件测试，必要时检查软件的设计开发、验证与确认文档，及以下方法来检验其是否符合要求：

——如适用，被测事务至少包括软件客户端用户登录、首幅影像加载和外部实体向被测软件检索影像列表；

——软件的时间特性测试应在随附文件中规定的影响变量的约束条件下进行；

——时间特性测试应在单一或制造商规定的并发下进行；

——当进行并发的时间特性测试时，应在每一个被测事务开始时设定集合点；

——在测试时间特性时，应关闭“预加载”等功能并清除缓存，如果预加载功能是不可关闭的，应在声称值和测试结果中均予以注明；

——如果开始与终止是基于操作者交互的，应以操作者交互输入的时间点作为开始时间，以向操作者完成预期输出的时间点作为终止时间；如中间过程存在操作者交互，应在结果中去除思考时间。

4.3.3 资源利用性

随附文件应给出软件在指定的运行环境下的资源利用性约束，至少包括平均 CPU 占用率。

通过检查随附文件、软件测试，必要时检查软件的设计开发、验证与确认文档，及以下方法来检验其

是否符合要求：

——软件的资源利用性测试在 4.3.1.1 与 4.3.2 的测试中同时进行；

——资源利用性测试监控的对象仅包括被测软件服务器端。

4.4 可靠性

4.4.1 数据备份与恢复

除了数据备份与恢复由被测软件之外的其他软件进行实现的情形外，应符合以下要求：

a) 随附文件中应分别列举产品的数据备份功能所能够备份的数据类型；

b) 随附文件应给出数据备份和恢复规程的信息；

c) 操作者执行备份数据的恢复操作时，如已有数据将被覆盖，软件应给出提示；

d) 无论何种情况下，当软件显示备份操作已被成功地执行了，则应成功生成相应的备份文件，并应可以用于恢复；

e) 恢复后的数据应与生成备份文件时的相应数据是一致的；

f) 基于 DICOM 协议的影像数据备份功能应支持 DICOM commitment SCU 服务；

g) 支持作为基于 DICOM 协议的备份目的地的软件应支持 DICOM commitment SCP 服务；

h) 非基于 DICOM 协议的影像数据备份功能应有方法判断本地存储的每一个影像数据是否已经被备份。这一功能在影像数据被修改后也应能正确实现。

通过检查随附文件、软件测试，必要时检查软件的设计开发、验证与确认文档，及以下方法来检验其是否符合要求：

——对于 b)中的要求，当数据备份或恢复是由其他软件进行实现时，可给出使用外部软件备份或恢复的必要指示(如：数据存放路径等)；

——对于 d)中的要求，测试时应考虑对相同数据的重复备份、系统可用空间不足时进行备份、对空数据进行备份等情形；

——对于 e)中的要求，测试时应考虑系统可用空间不足时进行恢复。

4.4.2 磁盘空间检测

软件应支持磁盘空间检测功能：

a) 软件应预设或支持由操作者设定磁盘空间不足的限值；

b) 当磁盘空间达到设定的限值时，应给出提示。

通过软件测试，必要时检查软件的设计开发、验证与确认文档，及以下方法来检验其是否符合要求：

——对于 b)中的要求，如果随附文件中没有定义限值的参考单位，测试时设定的边界值应精确到磁盘分配单元，否则应以随附文件中定义的值为准。

4.4.3 容错性

随附文件应陈述软件在接口、组件、系统或网络资源可用性引发差错的情况下继续运行(可用)的能力。

软件的容错性应符合随附文件中的陈述。

通过检查随附文件、软件测试，及必要时检查软件的设计开发、验证与确认文档来检验其是否符合要求。

4.4.4 软件稳定性测试

预期在指定的运行环境下不间断运行的软件应通过软件稳定性测试。

制造商应规定软件稳定性测试所执行的工作流和通过准则，通过准则应包括工作流成功率占比。

注：稳定性的通过准则还有可用时间占比、初始/终末性能效率比等，考虑评价的典型性和可行性，本文件推荐采用工作流成功率作为通过准则。

通过检查随附文件、软件测试，必要时检查软件的设计开发、验证与确认文档，及以下方法来检验其是否符合要求：

——在工作流执行中，应在关键节点处设置断言，以验证步骤的正确执行；

——加载指定数量的虚拟用户连续执行设计好的工作流，持续时间应累计至少为 24 h；

——工作流的执行成功率应被同时记录；

——当软件无法继续执行指定的工作流、崩溃或失去响应，视为稳定性测试失败；

——软件稳定性测试所使用的测试工具可以是基于图形化界面交互或模拟客户端请求的。

4.5 网络安全

4.5.1 自动注销

具有终端的软件应具备基于闲置时间的自动注销功能。

自动注销状态下，健康数据应不可见。

自动注销后，用户再次登录时，未保存的数据不应丢失，这个要求即便是再次登录的用户并非自动注销前的用户时也应满足。

自动注销后操作者应需要再次进行用户身份鉴别才能登录软件。

通过软件测试，必要时检查软件的网络安全相关文档，及以下方法来检验其是否符合要求：

——自动注销功能应在可设置的条件的最小边界值和由测试者选取的典型值进行测试，可在最大边界值进行测试；

——对于自动注销后的再次登录，使用与冷启动时登录软件所使用的不同的身份鉴别方式或凭证也被视为测试通过。

4.5.2 审计

软件应具有记录健康数据的调阅、修改和删除事件有关的审计信息的能力。

软件应在面向具有审计日志查阅权限的用户的文档中给出日志关键字信息，应包括所有日志关键字的含义、生成条件和生成格式。

审计日志应不可修改，所记录的信息应确保可以追溯到具体的用户、时间和事件。

如审计日志能够被软件发送给其他媒介或终端，应有方法确保传输过程的保密性和完整性。

通过软件测试，必要时检查软件的网络安全相关文档，及以下方法来检验其是否符合要求：

——测试用例的设计应遍历每一个日志关键字，以及在进行全部功能性、网络安全测试后查看文档中的日志关键字信息是否包含了所有网络安全日志；

——通过尝试对网络安全日志进行编辑、修改系统日期从而实现盖写等操作进行测试。

4.5.3 授权

软件应能对存储的影像进行访问授权，以控制用户仅能访问其有权限访问的影像。

软件在数据访问授权时，应考虑最小数据授权原则，仅提供完成预期用途所必需的健康数据的授权，或向用户提供实现该原则的必要设置选项。

预期用于访问指定患者影像的授权凭据不应仅使用与患者身份绑定的信息。

注：例如：使用完整的身份证号即可查阅对应患者的影像信息。

授权凭据不应硬编码于软件中。

每次从新设备访问需要进行授权的数据时，应要求用户重新提交授权凭据，即便这些数据是经由已被授权的用户转发的。

通过软件测试及必要时检查软件的网络安全相关文档来检验其是否符合要求。

4.5.4 节点鉴别

使用 DICOM 协议进行通信时，软件应能设置合法访问节点的应用实体名称（AE Title），宜能设置合法访问节点的 IP 地址、端口号等信息。

软件应支持对应用实体权限的控制。

注：如 C-FIND、C-MOVE、C-Store、Filming、MPPS、Worklist 等权限配置。

通过软件测试及必要时检查软件的网络安全相关文档来检验其是否符合要求。

4.5.5 人员鉴别

软件应支持对每一个用户提供各自的鉴权凭证。

对于使用额外的硬件进行人员鉴别时（如：指纹传感器、读卡器、虹膜传感器等），随附文件中应指定对鉴别设备的要求、与软件的连接方式以及如何加密。

通过软件测试及必要时检查软件的网络安全相关文档来检验其是否符合要求。

4.5.6 连通能力

随附文件中应指明使用本软件所必需的硬件连通能力。

随附文件中应给出软件占用的网络端口以及软件与其他软件、软件各组件之间的传输协议。

对于支持 DICOM 传输协议的软件，见 4.7.1。

通过检查随附文件、软件测试，必要时检查软件的网络安全相关文档来检验其是否符合要求。

注：对于硬件连通能力的要求，仅考虑必须具备的连接。

示例：当软件必须通过 USB 接口控制指定的医疗器械硬件时，USB 接口视为必需的硬件连通能力；当软件能够通过操作系统的文件 I/O 功能向 U 盘存储文件时，USB 接口不视为必需的硬件连通能力。

4.5.7 物理防护

以云服务形式交付的软件，随附文件中应指明部署环境的物理防护形式。

通过检查随附文件及必要时检查软件的网络安全相关文档来检验其是否符合要求。

4.5.8 系统加固

随附文件应就如何关闭或禁用软件运行所不需要的端口、通信协议、服务、应用程序或引导程序给出必要的说明。

以云服务形式交付的软件，随附文件应指明部署环境的等级保护级别。

通过检查随附文件及必要时检查软件的网络安全相关文档来检验其是否符合要求。

4.5.9 数据去标识化

将影像传输到软件之外（包括文件形式的传输行为和数据流形式的影像呈现行为）时，软件应具有去标识化的功能，去标识化字段应至少包括患者姓名、患者唯一标识、患者地理位置信息、患者联系方式、医疗机构名称、医疗机构地址。

去标识化功能宜进行分级，允许操作者选择需要的字段或预置的字段组合进行去标识化。

当影像的接收方是影像后处理应用程序，且其后处理结果预期仅回传给本软件时，应支持传输去标识化以及接收恢复标识化功能。

注：该功能可允许影像传输经过不受信任的网络、节点或终端时，将去标识化程度提升至最高。

通过软件测试及必要时检查软件的网络安全相关文档来检验其是否符合要求。

4.5.10 数据完整性与真实性

制造商应给出软件保障数据完整性的措施。

以非授权方式更改用户访问控制设置（包括用户名/密码表、密码尝试次数设置、用户权限设置等）、影像传输设置（包括节点白名单、传输协议设置、加密设置等）、影像存储设置（包括允许的存储形式、存储匿名机制等）的行为应：

——被阻止，或

——被识别并以适当的形式通知用户。

支持多家医疗机构共用云服务的软件，应能确保各个机构的数据隔离性、可靠性和完整性，并应能不受不同医疗机构的患者 ID、检查号重复的影响。

通过软件测试、必要时检查软件的网络安全相关文档，及以下方法来检验其是否符合要求：

——根据制造商给出的数据完整性保障措施设计测试用例进行测试。

4.5.11 数据备份与灾难恢复

当数据备份与恢复功能预期用于防范计算机系统遭到非预期的破坏时，随附文件应对备份数据的安全保存给出必要的信息。

备份与恢复功能的要求见 4.4.1。

通过检查软件的网络安全相关文档来检验其是否符合要求。

4.5.12 数据存储保密性与完整性

患者健康数据以及未去标识化的影像数据存储于公有云环境时，其内容应被加密。

软件应能识别出对用户授权数据、审计日志数据以及其他与网络安全能力有关的数据的完整性产生损害的事件，且能够提供记录这些事件并使授权用户获知的方法。

通过软件测试及必要时检查软件的网络安全相关文档来检验其是否符合要求。

4.5.13 数据传输保密性

患者健康数据以及未去标识化的影像数据通过公网传输时，传输过程应有加密措施。

患者健康数据以及未去标识化的影像数据通过局域网传输时，传输过程可具有加密措施。

通过软件测试及必要时检查软件的网络安全相关文档来检验其是否符合要求。

4.5.14 数据传输完整性

由操作者发起的，同时发送或接收多幅影像的行为应有影像序列完整性检查机制，并就完整性检查结果给出相应提示。

将数据通过公网进行传输的软件，应有确保影像及患者健康数据传输过程完整性的措施。

支持分布式存储或数据同步功能的软件，应能确保影像数据的一致性；检索和调阅时，对尚未同步的数据，应提供适当的状态指示。

通过软件测试及必要时检查软件的网络安全相关文档来检验其是否符合要求。

4.5.15 网络安全补丁升级

当软件预期不接入互联网时，随附文件应告知用户检查与执行运行环境及软件自身的安全缺陷修复程序的必要性。

通过检查随附文件及必要时检查软件的网络安全相关文档来检验其是否符合要求。

4.5.16 软件物料清单

软件应能显示已安装的所有组件及其版本信息。

当已安装的组件发生变化时，显示的组件及版本信息应相应更新。

通过软件测试及必要时检查软件的网络安全相关文档来检验其是否符合要求。

4.5.17 现成软件维护

随附文件应对软件所包含的现成软件及如何获取这些现成软件的网络安全更新给出必要的说明。

通过检查随附文件及必要时检查软件的网络安全相关文档来检验其是否符合要求。

4.5.18 网络安全指导

宜向承担不同级别的网络安全职责的操作者分别提供各自的随附文件。

注：医疗 IT 系统的管理员与医生承担着不同级别的网络安全职责。

随附文件应给出当用户发现产品的网络安全漏洞时，向制造商反馈的途径。

通过检查随附文件及必要时检查软件的网络安全相关文档来检验其是否符合要求。

4.5.19 网络安全特征配置

当任何一项网络安全要求的满足受到用户设置的影响时，随附文件应解释这些设置的方法与结果。

注：这些设置可能包括用户权限设置、去标识化设置和加密设置等。

通过检查随附文件及必要时检查软件的网络安全相关文档来检验其是否符合要求。

4.5.20 紧急访问

软件可具有紧急访问功能，以及在无用户授权的情况下访问软件的指定功能。

紧急访问可具有专用凭据，该凭据不被认为是用户访问控制机制的一部分。

如软件具有紧急访问功能：

——根据预期使用场景，紧急访问应通过适当的方式实现最小数据授权原则，以确保通过紧急访问功能登录的用户仅能访问预期使用场景中必要的影像。

示例 1：紧急访问时仅能访问新增数据，无法访问历史数据。

示例 2：紧急访问时需要通过一个或多个精确条件进行检索方能访问符合条件的数据，不支持空的检索条件以及模糊的检索条件。

——紧急访问行为、使用的凭据以及所访问的影像数据应有审计日志记录。

——可支持禁用紧急访问功能。

通过软件测试及必要时检查软件的网络安全相关文档来检验其是否符合要求。

4.5.21 远程访问与控制

应使用不低于 32 bit 真彩色或 8 bit 灰阶的方式提供预期用于诊断的远程影像显示。

当远程影像显示不满足色彩、灰阶、分辨率的最低要求时，应给出提示。

当使用灰阶方式提供远程影像显示时，随附文件中应给出有诊断价值的信息可能会丢失的说明。

通过软件测试及必要时检查软件的网络安全相关文档来检验其是否符合要求。

4.5.22 恶意软件探测与防护

以云服务形式交付的软件，随附文件中应指明部署环境所使用的恶意软件探测与防护软件及其引

擎与特征库版本的查看方法。

除非以非 DICOM 格式存储影像数据或将影像数据直接以二进制形式存储在数据库中，软件应有 DICOM 导言内容鉴别机制：

——直接将所有导言内容置为 00H；

——或以白名单的形式将允许的导言内容保留，将白名单以外的导言置为 00H；

——或能鉴别可执行类型的导言内容，将其置为 00H。

这个鉴别机制可以发生在接收/导入影像数据时或发送/导出影像数据时。

通过检查随附文件、软件测试及必要时检查软件的网络安全相关文档来检验其是否符合要求。

4.6 维护性

4.6.1 维护性日志

软件应具有维护性日志记录与软件维护有关的信息。

软件应在随附文件或用于软件维护人员阅读的文档中给出日志关键字信息，应包括所有日志关键字的含义、生成条件和生成格式。

通过检查相应文档、软件测试及必要时检查软件的设计开发、验证与确认文档来检验其是否符合要求。

4.6.2 软件状态的指示

随附文件中应对与软件维护有关的软件运行状态的每个指示给出解释说明，以及必要时给出可能导致的结果。

注：软件运行状态的指示可能包括用于诊断产品的缺陷或失效原因的提示。

通过检查随附文件及必要时进行软件测试来检验其是否符合要求。

4.6.3 远程维护

随附文件中应声明软件支持的远程维护功能，该要求同样适用于经过制造商验证的第三方远程维护工具提供的功能。

通过检查随附文件及必要时进行软件测试来检验其是否符合要求。

4.6.4 软件升级

支持由用户进行在线升级的软件，除了以云服务形式交付的软件以外，在执行软件升级时应由指定的用户进行确认并给出获取升级前后的版本及变化内容信息的方法。

通过软件测试来检验其是否符合要求。

4.7 兼容性

4.7.1 DICOM 兼容性

对于符合 DICOM 标准的软件：

a) 随附文件中应包含 DICOM 符合性声明；

b) 对于支持使用 DICOM 标准协议进行数据传输的软件，应能与相应的 DICOM 应用实体正确地进行通信；

c) 对于支持将影像信息存储为 DICOM 格式文件的软件，所存储的 DICOM 文件的每一个标准定义的元数据应符合 DICOM 符合性声明中涉及的要求。

通过检查 DICOM 符合性声明及软件测试来检验其是否符合要求。

对于b)中的要求，测试环境的部署应包括被测软件支持进行通信的每种类型的DICOM应用实体。

当软件所存储的文件的元数据均由其他应用实体创建时，c)中的要求不适用。

4.7.2 必备软件兼容性

如随附文件中指明软件能与其他医疗器械软件互操作，应能正确按照随附文件中定义的行为进行通信。

通过检查随附文件、软件测试，及必要时检查软件的接口文档来检验其是否符合要求。

4.7.3 必备硬件兼容性

如随附文件中指明软件能与某必备医疗器械硬件兼容(如医用影像设备)，应进行兼容性测试。

通过检查随附文件、软件测试，必要时检查软件的接口文档，及以下方法来检验其是否符合要求：

——必备硬件兼容性测试用例应覆盖所有与必备硬件的接口/交互功能。

4.7.4 组件兼容性

如果软件允许用户进行安装，应提供一种方式来控制已安装组件的兼容性。

软件应能识别出哪个组件负责兼容性。

通过软件测试来检验其是否符合要求。

4.8 可移植性

4.8.1 运行环境

随附文件中应给出软件的运行环境，至少包括软件环境、最低的硬件环境和最低的网络环境。

当软件的组件分别运行在不同的计算机系统时，每一个计算机系统的运行环境应分别给出。

当对于软件的一个或多个组件而言有多个可选择的运行环境时，随附文件应陈述允许的每种组合。

对于支持用于显示的医学影像云服务的软件，应有操作者需确认终端是否符合医学影像显示系统的要求的提示或提供预置的用于医学影像显示系统符合性测试的标准图形。

注：对于医学影像显示系统，参见YY/T 0910.1。

通过检查随附文件、软件测试及以下方法来检验其是否符合要求：

——当软件的一个或多个组件的软件环境中相同的项具有多个版本的组合时，测试时应考虑其中一项取最高版本而其他所有项皆取最低版本的每一种组合情形。

4.8.2 安装与卸载

如果软件允许用户进行安装，遵循随附文件中的信息应能成功安装并运行软件。

单机软件和基于C/S架构的客户端软件应向用户提供卸载方法。

通过检查随附文件及软件测试来检验其是否符合要求。

附 录 A
（资料性）
测量功能的不确定度评定

对于软件的测量功能而言，其结果受到很多随机因素与系统因素的影响，通过对这些因素进行识别并进行不确定度评定，可以对测量结果的质量给出定量的评价。

从测量结果的产生过程来看，其不确定度贡献主要来自两个主要方面：

a) 扫描设备和扫描物产生的输入量 $X_{a,1}$，$X_{a,2}$，…，$X_{a,N}$（例如：CT 设备所给出的像素间距、DR 影像中的标准球体的直径等）贡献的不确定度分量 $u(x_{a,i})$；

b) 由软件和运行环境的设置与使用产生的输入量 $X_{b,1}$、$X_{b,2}$，…，$X_{b,N}$（例如：图像在屏幕中所显示的分辨率、计算时的数据精度、连续值与离散值的映射等）贡献的不确定度分量 $u(x_{b,i})$。

其中，a)中的不确定度分量往往与测量软件无关，但对于测量软件的用户而言，其所感知的测量结果的质量无疑与该不确定度分量相关。在软件的随附文件中单独对这些不确定度分量给出识别和说明，有利于用户正确理解整个测量系统的不确定度构成和在评定整个测量系统的不确定度时给予必要的提示。

b)中的不确定度分量中，有些是固化于软件的编码中的，而另外一些则与软件和运行环境的设置、操作者对软件的操作相关。制造商有责任在随附文件中对这些不确定度分量的计算方法或不确定度评价中的关键信息（例如：输入量之间的函数关系、输入量的概率分布等）进行说明，以便用户遵循这些说明能够实现对相应不确定度分量进行充分识别与正确评价。

最终的测量结果 Y 的计算是由测量软件给出的，其由各个输入量通过函数关系 f 来确定：

$$Y=f(X_{a,1},X_{a,2},\cdots,X_{a,N},X_{b,1},X_{b,2},\cdots,X_{b,N}) \qquad \cdots\cdots\cdots\cdots(A.1)$$

用户可以通过随附文件中给出的函数关系 f 对软件测量结果的合成标准不确定度进行计算，并计算给定包含因子下的扩展不确定度。

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 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

[3] GB/T 27418—2017 测量不确定度评定和表示

[4] GB/T 35273—2020 信息安全技术 个人信息安全规范

[5] YY/T 0910.1—2021 医用电气设备 医学影像显示系统 第1部分:评价方法

[6] ISO/IEC/IEEE 24765:2017 Systems and software engineering—Vocabulary

[7] 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

中华人民共和国医药
行业标准
医学影像存储与传输系统软件
专用技术条件
YY/T 1861—2023
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 1.5 字数 44 千字
2023年1月第一版 2023年1月第一次印刷
*
书号:155066·2-36786 定价 36.00 元

如有印装差错 由本社发行中心调换
版权专有 侵权必究
举报电话:(010)68510107

YY/T 1861-2023

码上扫一扫 正版服务到