发 布

国家药品监督管理局

20XX—XX—XX实施

20XX—XX—XX发布

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

（征求意见稿）

YY/T XXXX-XXXX

中华人民共和国医药行业标准

YY

ICS 11.040.50

C 43

前  言

本标准按照GB/T 1.1—2020给出的规则起草。

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这些专利的责任。

本部分由国家药品监督管理局提出。

本部分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/TC10/SC1）归口。

本部分起草单位：

本部分主要起草人：

医学影像存储与传输系统软件专用技术条件

1 范围

本标准规定了医学影像存储与传输系统软件的术语和定义、要求和试验方法。

本标准不适用于：不使用DICOM协议的心电图、内窥镜、病理学、眼科学、超声学、皮肤病学以及牙科学影像存储与传输系统。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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 25000.10-2016 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 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

ISO 12052-2017 Health informatics — Digital imaging and communication in medicine (DICOM) including workflow and data management

GB 18030信息技术 中文编码字符集

GB/T 10149医用X射线设备术语和符号

GB/T 35273-2020信息安全技术 个人信息安全规范

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

IEC/TR 80001-2-2：2012Application 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

3 术语和定义

GB/T 10149、GB/T 25000.10-2016界定的以及下列术语和定义适用于本文件。

医学影像存储与传输系统软件

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。

DICOM

医学数字成像及通信



渐进式加载

加载影像时，首先显示低分辨率的影像，待影像全部加载完成后再显示完整分辨率的影像。

数据冲突

对于某项特定的数据存在两个不同的值的状态。

断言 Assertion

一种放在测试脚本中的一阶逻辑（如一个结果为真或是假的逻辑判断式），目的是为了标示与验证测试者预期的结果。

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。

影像视窗 image view port

用于显示影像的最小界面单元。

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。

像素 pixel

二维数字影像中的最小显示单位

体素 voxel

三维数字影像中的最小体积单位

操作者 operator

操作软件的人。

注：对于软件而言，具有相同访问凭据的用户被视为相同的操作者。

[来源：GB 9706.1-2020，有修改]

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，有修改]

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，有修改]

明示指示

使操作者不需要进行任何额外操作便能阅读，且能够明确地告知操作者当前软件的某项状态、当前需要进行的操作或可供选择的选项及其对应后果的消息。

布局 layout

界面的展现形式

医学影像云服务（云服务）

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。

最大并发事务数

软件能够承受的同时接收到的事务数的极限，超过该事务数，将导致系统吞吐量下降，并可能导致软件崩溃、失效。

事务吞吐容量

在单位时间内软件能够处理完成的事务量，单位是TPS或TPM。

影像处理容量

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。

（请求）安全

不会修改资源状态的请求特性

（请求）幂等

多次调用返回的效果（形式）一致的请求特性

健康数据 health data

与身体或心理健康相关的个人敏感数据。

注：由于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或法规。

[来源：IEC/TR 80001-2-2：2012，定义3.7，有修改]

匿名化 anonymization

通过对个人信息的技术处理，使得个人信息主体无法被识别或者关联，且处理后的信息不能被复原的过程。

[来源：GB/T 35273-2020，3.14]

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]

标注标识

叠加在影像上用于标示与位置有关的发现、测量结果、测量基准的文字或符号

感兴趣区域 ROI

用于划定影像中点、区域与体积的标注标识

影像附加信息

属于某一影像的患者信息、影像参数信息和其他信息。

1. 要求
   1. 随附文件的通用要求

4.1.1 如适用，软件的随附文件应陈述下列信息：

1. 其自身的唯一标识；
2. 软件预期使用者应当具备的知识背景；  
   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；  
   ——中文以外的其他语言。
3. 软件是否允许用户进行安装操作；
4. 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；
5. 软件中的已知存在缺陷的功能；
6. 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；
7. 软件产品的边界；

注：通常可以用与本软件之外的软件的接口来定义。

1. 软件组件的选项和版本；
2. 用户可调用的接口和相关的被调用软件；
3. 软件支持的语言；
4. 术语和缩略语的定义；
5. 软件的载体；

通过检查随附文件来检验是否符合要求。

4.1.2 随附文件不应自相矛盾、互相矛盾以及与软件相矛盾。

通过检查随附文件、软件测试来检验是否符合要求。

* 1. 功能性与易用性
     1. 通用要求

随附文件应陈述操作者能够使用的所有软件功能。

随附文件中陈述的软件功能应当是可测的或可验证的。

除了已经写明的已知缺陷外，软件功能应当符合随附文件中对软件功能的描述。

随附文件应陈述用户可能碰到的所有已知的限制；

软件中用于标记的符号，其含义应在随附文件中解释。

除非在与用户交互时提供明示指示，软件中每一用户交互元素的含义应在随附文件中解释。

每个软件出错消息应指明如何改正差错或向谁报告差错。

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。

注：用户交互元素包括按钮、菜单、视窗、快捷键等。

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。

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、软件测试及必要时检查软件的设计开发、验证与确认文档来检验是否符合要求。

随附文件中说明的所有功能、使用限制，以及待完成的任务的代表性的功能组合，均应经测试用例测试。

* + 1. 影像接收与发送

1. 如适用，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；
2. 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做以明显区分；
3. 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；
4. 软件应符合随附文件对影像接收与发送行为的陈述；
5. 软件应给出处于影像接收与发送状态的指示；
6. 当软件处于影像接收与发送状态时，关闭软件应有需要操作者确认的明示指示；
7. 当软件支持将影像归档到上一级或更长期的存储系统时，应有方法确认每一个影像是否已经被归档。

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是否符合要求。

* + 1. 影像附加信息

软件可支持操作者录入和接口传入（以下简称为录入和传入）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：

1. 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；
2. 对于姓名及健康数据文本的录入与显示应支持中文，封装字符集应支持GB18030。
3. 应当在随附文件中给出影像附加信息的录入和传入限制；

注：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。

1. 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明示指示，且允许操作者对其再次编辑；
2. 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明示指示；
3. 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当被检索功能完全覆盖；
4. 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当立即更新。

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，应当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，同样应当对参数表进行上述检查。

* + 1. 影像导入与导出

1. 软件应能按照数据传输与储存规范进行影像导入与导出。
2. 软件应给出影像导入状态的指示，其形式可以是进度条、状态标记、虚拟指示灯等。
3. 影像导入失败时，软件应给出明示指示。
4. 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。
5. 如影像导入伴随着附加信息的导入，后者应符合4.1.3的要求。
6. 当导出目的地存在同名文件或文件夹时，软件应给出明示指示、自动重命名文件或允许操作者再次选择目的地。
7. 当导出为有损影像时，界面上应有明示指示。
8. 随附文件中应当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、软件测试及必要时检查软件的设计开发、验证与确认文档来检验是否符合要求。

影像导入失败的测试用例应包括：存储空间不足、数据传输中断、超时、校验和错误等。

导入影像格式的测试用例应包括：错误的扩展名、空扩展名、伪造的文件头等。

* + 1. 影像索引及调阅服务

1. 软件应支持对内部或对外部的影像索引及调阅服务。
2. 宜支持对不同目标分别定义可索引及调阅的影像范围。

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是否符合要求。

* + 1. 影像存储与访问

a) 随附文件应指明软件存储影像的方式为无损存储、有损存储或二者都使用。当使用了无损存储时，存储影像与原始影像像素值均方误差应满足：

MSE≤1×10-6。

注：仅比较影像的一致性，不包括影像附加信息。

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，应当提供数据锁功能，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、传输或删除上锁的数据时，应有明示指示；

e) 数据锁应当可以由上锁操作者、管理员或适当时自动解除；

f) 当数据锁不能够随着第一个编辑数据的操作者的访问自动执行时，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、软件测试及必要时检查软件的设计开发、验证与确认文档来检验是否符合要求。

均方误差的计算：设原始影像为{g(x,y),0≤x≤M-1,0≤y≤N-1}，存储至PACS软件并读取出的影像为{f(x,y),0≤x≤M-1,0≤y≤N-1}，则按下式计算均方误差：

患者信息冲突的测试用例应当包括操作者录入信息冲突、影像存储（归档）时冲突、从文件tag中自动读取患者信息时冲突等。

* + 1. 影像合并

a) 对于支持影像合并功能的软件，应当在合并前进行检查，当可能存在将不同患者数据进行合并时应给出明示指示。

b) 对于重复的影像，合并时应当分别存储或让操作者选择是否覆盖。

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是否符合要求。

影像合并的测试用例应当包括除指定的uid（唯一编号）以外其他每项字段重复的情形，还应当包括每项字段为空的情形。

* + 1. 影像显示

对于支持影像显示的软件，应符合以下要求：

a) 随附文件中应当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) 应当支持显示影像的平移、翻转功能。

c) 应当支持显示影像的缩放功能。

d) 应当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，应当支持在序列内进行影像滚动翻页的功能。

f) 对于支持MPR重建的软件，应当支持显示定位线和重建层厚大小的功能。

g) 对于支持导入或接收影像图层上的叠加信息的软件（例如：DICOM GSPS标记），应当支持对其进行显示。

h) 对于支持多屏幕显示的软件，应当能有方法使影像显示在用于诊断的屏幕上。

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是否符合要求。

影像显示支持测试所使用的数据应当包括标准影像文件、影像显示条件信息以及预期的显示效果。

对于影像显示的测试用例，应当对每一个支持的影像模态进行所有要求的测试。

* + 1. 测量功能

a) 随附文件应给出软件各项手动测量功能的最大允许误差。

b) 如适用，测量精度应当在轴位影像、MPR重建的冠状位、矢状位及斜切位影像以及CPR重建的展开面进行测试

c) 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。

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像素与影像像素应能区分。

f) 如软件支持在三维影像中进行测量，应当在随附文件中给出三维影像测量选点时垂直于视窗平面方向的坐标定位机制，并应加以验证。

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是否符合要求。

应遍历每个功能不同的测量工具（对于同一功能的测量工具，不需遍历工具的每种配置。例如对于直径线性可调的涂抹工具，不需要遍历每种画笔直径。）

测量应当在随附文件中定义的最低运行环境下进行，可以使用几何尺寸可溯源的真实物体的影像或使用像素尺寸与几何形状被充分定义的数字影像进行验证。

* 1. 性能效率
     1. 容量
        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（TPS）与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%。

如适用，测试工作流应当至少包括：

a) 被测软件客户端的用户登录、查询、首幅影像加载；

b) 外部应用实体向被测软件存储（归档）影像；

c) 外部应用实体向被测软件检索影像列表，并获取影像。

软件的最大并发事务数、事务吞吐量及事务成功率应符合随附文件中的要求。

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是否符合要求。

推荐的测试典型影像：512×512重建矩阵、12bit存储位深、含有200幅影像的CT序列。

当存在缓存时，最大并发事务数测试应当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，应当对事务吞吐量以及事务的成功率进行监控。

在测试中不应设置集合点。

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5min。

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，如前者的吞吐量小于等于后者，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。

* + - 1. 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、软件测试及必要时检查软件的设计开发、验证与确认文档来检验是否符合要求。

* + 1. 时间特性

随附文件中应给出软件在指定的运行环境下的时间特性，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；

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。

使用分布式存储的医学影像云服务软件，发起同步请求的间隔不应大于10s

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是否符合要求。

软件的时间特性测试应当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，应当在每一个被测事务开始时设定集合点。

在测试时间特性时，应当关闭“预加载”等功能并清除缓存，如果预加载功能是不可关闭的，应当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，应当以操作者开始发起交互的时间点作为开始时间，以操作者交互完整显示的时间点作为终止时间。如中间过程存在操作者交互，应当在结果去除这些操作者交互前的思考时间。

时间特性的测试结果应符合随附文件中的要求

* 1. 可靠性
     1. 数据删除

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，软件应当要求操作者确认，并提供取消该操作的功能，或可撤销删除操作。

对于文本编辑中的删除操作，可不给出提示，宜提供撤销功能。

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，并需要操作者配置明确的删除条件后方可执行。

对一定时间之前的影像具有自动删除功能的软件，应有机制判断系统时间是否被错误地修改，这一机制可以是与上一次正确启动软件时的时间进行对比或基于其他可获得的时间基准进行对比。当用做比较的影像时间为空、为未来时间或早于软件部署的时间时，自动删除行为应被阻止或由操作者确认方可进行。

如果软件对已归档的数据具有自动删除功能（无论这个功能是否有其他规则限制），应能判断归档到其他存储的请求是否已成功执行。（通过DICOMCommitment或其他可以确认成功归档的方式。）

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是否符合要求。

设计的测试用例应包括：

a) 遍历所有具备删除权限的角色，如果这些角色中的删除权限是复用的（例如：删除权限作为单独的配置项存在）则仅选择其一进行测试。

b) 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。

c) 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。

注：以上遍历不包括条件间的组合，在设计用例时，应当设计合适的条件组合以覆盖上述要求，但无需遍历每种组合。

* + 1. 数据备份与恢复

1. 随附文件中应分别列举产品的数据备份功能所能够备份以及不能够备份的数据类型；
2. 随附文件应给出数据保存和恢复规程的信息；
3. 操作者执行备份数据的恢复操作时，如已有数据将被覆盖，软件应当给出明示指示；
4. 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；
5. 恢复后的数据应与生成备份文件时的相应数据是一致的。

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是否符合要求。

设计的测试用例应包括：

对相同数据的重复备份

系统可用空间不足时进行备份

系统可用空间不足时进行恢复

对空数据进行备份（如软件通过安装程序、实施规程或指定的脚本确保初始化的可备份数据库不会为空，且无法手动清空，则无需设计此用例）

* + 1. 诊断影像误用的防止

1. 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，应有明确的指示进行区分
2. 当序列是由其他后处理功能生成而非扫描的原始影像时（例如：通过MPR重建所得的影像），应有方法对这些影像进行区分。
3. 如软件具有渐进式加载功能，应当在影像未达到完整分辨率时给出明示指示，且无法使用需要完整分辨率影像的工具。
4. 当前系统所设置的屏幕分辨率以及UI缩放不能满足软件规定的范围时，应给出提示。
5. 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。
6. 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，应当指明当前非真实尺寸的显示状态。
7. 对于当前显示的使用了有损压缩的影像，应由操作者进行选择或有明示指示
8. 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，应有明示指示并在随附文件中说明。

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是否符合要求。

* + 1. 磁盘空间检测

a) 软件应对磁盘空间进行检测并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，应给出明示指示。

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是否符合要求。

在设计磁盘空间检测测试用例时，设定的边界值应当精确到分配单元。

* + 1. 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。

软件的运行应符合随附文件中关于容错性的陈述。

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是否符合要求。

* + 1. 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测试所执行的工作流和通过准则，通过准则可包括软件可用时间占比或工作流成功率占比。

软件应符合制造商规定的稳定性测试通过准则。

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是否符合要求。

1. 在工作流执行中，应当在关键节点处设置断言，以验证步骤的正确执行。
2. 加载指定数量的虚拟用户执行设计好的工作流，持续时间应累计至少为168h。
3. 工作流的执行成功率应被同时记录。
4. 在设计工作流时，应当考虑到软件失效的情形，并设计相应的恢复措施，这个恢复措施可以是逐级尝试的（例如重启服务端软件-重启服务器-恢复默认的配置文件-恢复数据库-运维人员手工介入恢复）
5. 当预先设计的任何恢复措施都无法恢复软件运行时，视为稳定性测试失败。
6. 当可由一个恢复措施恢复软件运行时，恢复运行所需的总累积时间应被记录为软件不可用时间。
7. 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。
   1. 网络安全
      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当满足。

自动注销后操作者应当需要再次进行用户身份鉴别才能登录软件（这个身份鉴别凭证可能是与冷启动时登录软件所使用的不同的）。

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是否符合要求。

自动注销功能应当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。

* + 1. 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，应当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，所记录的信息应当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，应当有方法确保传输过程的保密性和完整性。

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是否符合要求。

测试用例的设计应当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。

* + 1. 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须的健康数据的授权，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，应当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是否符合要求。

* + 1. 网络安全特征配置

无通用要求。

* + 1. 网络安全补丁升级

无通用要求。

* + 1. 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，软件应具有匿名化的功能，匿名字段应至少包括姓名与患者ID。

匿名化功能宜进行分级，允许操作者选择需要的字段或预置的字段组合进行匿名化。

当影像的接收方是影像后处理应用程序，且其后处理结果仅回传给本软件时，应支持传输匿名化以及接收去匿名化功能。

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，将匿名化程度提升至最高。

当所传输的影像具有患者面部容貌等能够追溯到患者身份的信息时（例如：头部CT、MR影像），软件宜提供在不损失诊断所需信息的情况下去除影像中能够追溯到患者身份的信息。

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是否符合要求。

当一个软件指明了其运行的必备软件或作为底层运行环境的软件时，在此条款中它们可以被视为一个整体。

* + 1. 数据备份与灾难恢复

软件应具有影像数据备份功能。

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

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。

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。

通过软件测试及必要时检查软件的网络安全相关文档来检验是否符合要求。

* + 1. 紧急访问

软件可具有紧急访问功能，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。

例如：

——紧急访问时仅能访问新增数据，无法访问历史数据。

——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。

应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是否符合要求。

* + 1. 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

——应被识别并以适当的形式通知用户。

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。

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。

* + 1. 恶意软件探测与防护

以SaaS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影像数据时或发送影像数据时。

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是否符合要求。

* + 1. 节点鉴别

使用DICOM服务进行通信时，软件应能设置合法访问节点的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AE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是否符合要求。

* + 1. 人员鉴别

软件应当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），随附文件中应当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是否符合要求。

* + 1. 物理防护

以SaaS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是否符合要求。

* + 1. 现成软件维护

无通用要求。

* + 1. 系统固化

无通用要求。

* + 1. 网络安全指导

无通用要求。

* + 1. 存储保密性

患者健康数据以及未匿名化的影像数据存储于公有云环境时，其内容应被加密。

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是否符合要求。

* + 1. 传输保密性

患者健康数据以及未匿名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匿名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是否符合要求。

* + 1. 远程访问与控制

如适用，应使用不低于32bit真彩色或8bit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，应有明示指示。

当使用灰阶方式提供远程影像显示时，随附文件中应指明会丢失的有诊断价值的信息。

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是否符合要求。

* + 1. 抗拒绝服务攻击

以SaaS形式交付的软件，随附文件中应指明抗拒绝服务设备的部署方式、吞吐量以及支持防范的DDOS攻击类型。

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是否符合要求。

* 1. 维护性
     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，应当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是否符合要求。

测试用例的设计应当遍历每一个日志关键字，以及在进行全部功能性测试后查看文档中的日志关键字信息是否包含了所有维护性日志。

* + 1. 软件状态的指示

随附文件中应对软件运行状态指示器的每个指示给出解释说明，包括它们是如何触发的，以及必要时给出可能导致的结果。

通过检查随附文件及必要时进行软件测试来检验是否符合要求。

* + 1. 远程维护

如适用，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是否符合要求。

* + 1. 软件升级

支持在线升级的软件，在执行软件升级时应由指定的用户进行确认并通知用户升级前后的版本及变化内容信息。

通过软件测试来检验是否符合要求。

* 1. 兼容性
     1. DICOM兼容性

对于符合DICOM标准的软件，应当提供DICOM符合性声明，该文档应作为随附文件的一部分并有唯一标识。

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应用实体正确进行通信。

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是否符合要求。

对于涉及到使用DICOM协议进行数据传输的功能，应当用合适的测试工具模拟测试场景中其他所有的DICOM应用实体。

* + 1. 必备软件兼容性

如随附文件中指明软件能与其他RIS/HIS软件、其他医用信息系统或处理软件兼容，软件应能正确与该软件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是否符合要求。

* + 1. 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），应当进行兼容性测试。

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是否符合要求。

兼容性测试用例应当覆盖所有与必备硬件的接口/交互功能

* + 1. 运行环境

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

对于支持横向扩展的软件，运行环境应当以最小单元的形式给出。

对于部署在虚拟化环境下，且不允许用户对软件进行部署操作的软件，随附文件中可提供简化的运行环境要求，硬件环境至少包括CPU的核心数、内存、硬盘类型信息。

对于支持移动端影像调阅并预期用于诊断的软件，应当有明示指示指明操作者需确认终端是否符合医学影像显示的要求。

通过检查随附文件及软件测试来检验是否符合要求。

* + 1. 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。

软件应能识别出每一个已安装的组件的发布版本。

通过软件测试来检验是否符合要求。

* 1. 可移植性

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所有已安装的组件的方法。

通过检查随附文件及软件测试来检验是否符合要求。

对于软件应用程序的成功安装和正确运行，应就随附文件中列出的所有支持的平台和系统加以证实。