ICS 11.040.50
C43

YY

中华人民共和国医药行业标准

YY/T XXXX.1—XXXX

医用诊断X射线影像设备连通性符合性基本要求 第1部分：通用要求

Basic requirements of communication and comformance for medical X-ray image equipment Part 1: General requirements

点击此处添加与国际标准一致性程度的标识

（征求意见稿）

XXXX-XX-XX 发布　　XXXX-XX-XX 实施

国家药品监督管理局　　发布

目　　次

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

YY/T XXXX.1-XXXX《医用诊断X射线影像设备连通性符合性基本要求》分为如下部分：

——第1部分：通用要求；

——第2部分：X射线计算机体层摄影设备；

——第3部分：数字化摄影X射线机（DR）；

——第4部分：数字减影血管造影X射线机（DSA）；

——第5部分：乳腺X射线机；

——第6部分：口腔X射线机。

本部分为YY/T XXXX的第1部分。

请注意本文件的某些内容可能会涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由国家药品监督管理局提出。

本标准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。

本标准起草单位：

本标准主要起草人：

引　言

医用X射线影像设备连通性是一个广义的概念，它表达了医用X射线影像设备如何安全地、有效地存储及传输健康数据的能力。

随着医用X射线影像设备应用场景的不断拓展，医用X射线影像设备在临床得到广泛应用，同一组X射线诊断图像在不同的设备上的使用需求不断增强，医用X射线影像设备不论是单机使用，还是在局域网、广域网中使用，其软件组件的正确运行对于医用X射线影像设备的安全性、有效性至关重要。因此，本标准基于ISO 12052:2017健康信息学-医学数字成像和通讯(DICOM)包括工作流程和数据管理（Health informatics——Digital imaging and communication in medicine (DICOM) including workflow and data management）、IEC/TR 80001-2-2:2012 包含医疗设备的IT网络的风险管理应用 第2-2部分 医疗设备安全需求、风险和控制的披露和通报指南) (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)、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，给出了医用X射线影像设备及其相关软件组件连通性符合性的基本要求，包括了：兼容性、可靠性、网络安全、维护性、可移植性。

对于兼容性的要求，本标准基于国际标准ISO 12052标准中定义的DICOM协议的符合性，明确了医用X射线影像设备是否符合制造商所公布的DICOM符合性声明来验证其在临床应用中的互联互通性。

对于网络安全的要求，本标准基于IEC/TR 80001-2-2，结合了医用X射线影像设备的特性，将医用X射线影像设备理解为一个网络中的节点。

本标准中各条款的要求基于医用X射线影像设备在健康的网络环境当中，对于网络环境的部署和安全评估，并不在本标准的要求范围内。

医用诊断X射线影像设备连通性符合性基本要求
第1部分：通用要求

1 范围

本标准规定了医用X射线影像设备及其相关软件组件连通性符合性的通用要求、试验方法。

本标准适用于具有可存储或传输健康数据功能的医用X射线设备及其相关软件组件，本标准不适用于无存储和传输健康数据功能的医用X射线设备及其相关软件组件。

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 15532-2008 计算机软件测试规范

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

IEC TR 80001-2-2:2012包含医疗设备的IT网络的风险管理应用 第2-2部分 医疗设备安全需求、风险和控制的披露和通报指南（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）

ISO 12052:2017健康信息学-医学数字成像和通讯(DICOM)包括工作流程和数据管理（Health informatics—Digital imaging and communication in medicine (DICOM) including workflow and data management）

3 术语和定义

GB/T 10149-1988界定的以及下列术语和定义适用于本文件。

3.1 最终用户 end user

最终受益于系统结果的单独个体。

[GB/T 25000.1-2010，定义4.14]

3.2 健康数据 health data

表明身体或心理健康的隐私数据。

[IEC TR 80001-2-2:2012 定义3.7]

注：医学影像是一种典型的健康数据。

3.3 隐私数据 private data

与已识别或可识别的个人相关的任何信息
[IEC TR 80001-2-2 定义3.15]

3.4 预期用途 intended use

按照制造商提供的规范、说明书和信息，对产品、过程或服务的预期使用。
[YY/T 0316-2016，定义2.5]

3.5 制造商 manufacturer

对产品的设计、制造、包装或标记，对产品的组装，或对产品的改动负责的自然人或法人，不论这些活动是由其还是代表其的第三方执行。

注：改写自IEC 60601-1:2012，定义3.55。

4 通用要求

4.1 兼容性

4.1.1 DICOM 符合性

制造商应提供DICOM符合性声明。

注1：DICOM 符合性声明定义了医用 X 射线设备所支持的 DICOM 协议的实现，是医用 X 射线设备的影像能否相互兼容的重要参考，因此 DICOM 符合性声明应符合 DICOM PS 3 中的第二部分。如适用，也应符合本系列标准中其他部分的特定要求。

注2：符合性声明允许使用者确定特定的医用诊断 X 射线影像设备支持 DICOM 标准的哪些可选部分，以及医用诊断 X 射线影像设备附加了哪些附加的扩展或专有的 SOP 类。使用者可以通过比较两个不同的医用诊断 X 射线影像设备的符合性声明，确定两者之间是否有通讯支持及支持程度，以便进行更恰当的医疗用途。

注3：一个声称符合 DICOM 标准的医用诊断 X 射线影像设备不一定需要使用 DICOM 标准的所有可选择部分。在满足最低的通用要求的基础上，一个符合 DICOM 的医用 X 射线影像设备可能会使用完成既定任务所需的 SOP 类，通讯协议，介质应用框架文件，可选择（Type3）属性，编码及受控术语等。此外，DICOM 标准允许一个医用 X 射线影像设备扩展或专有化 DICOM 定义的 SOP 类，以及定义私有 SOP 类。

注4：DICOM 标准内容概述参见附录 A。

4.1.2 安全软件

如果产品可由用户进行软件安装的操作，制造商应规定产品与安全软件的兼容性，这样的规定应在随机文件中陈述，并应对制造商规定的安全软件进行兼容性验证。

注：安全软件一般包括杀毒软件、辅助安全软件和反流氓软件等。

4.2 可靠性

4.2.1 容错性

当网络数据传输中断时，健康数据不应丢失。

注：传输中断的原因应考虑来自网络异常、失去电源、使用者错误的操作、应用程序自身逻辑出错等。

4.2.2 易恢复性

当数据传输过程中，若响应时间超出了通常的预期限度，应告知最终用户。

注：实际测试时，宜考虑系统响应超时的时间在是否合理的范围内，这需要对设备实际的应用场景进行评估。

4.2.3 数据丢失的防止

产品在随机文件陈述的正常工作条件下使用时，健康数据不应丢失。

注：以上要求即使在下面的情况下也要满足：

——利用的存储容量达到制造商规定的极限；

——试图利用超出制造商规定极限的存储容量；

——最终用户造成的非预期的输入。

4.3 网络安全

4.3.1 保密性

4.3.1.1 存储保密性

制造商应在随机文件中陈述健康数据的存储是否被加密；若制造商提供了存储加密的手段，这种手段应是可用的。

注：责任方应根据当地法规要求通过控制设备的访问以确保数据保密性，并考虑本地数据存储保密的必要性。

4.3.1.2 传输保密性

当设备在进行网络数据传输时，应使用节点认证的方式(例如：白名单、用户名口令、证书等)；当设备在公用网络进行网络数据传输时，应提供确保传输过程中健康数据保密性的手段。

4.3.1.3 患者隐私的保护

若健康数据可以被导出，尤其是包含了可能识别患者身份的隐私信息，应提供保护其隐私性的手段。

注1：例如这样的隐私信息通常包括了：

——患者姓名；

——患者地理位置信息；

——患者联系方式；

——患者唯一标识；

——患者照片。

注2：数据的匿名化功能属于保护患者隐私性的手段的一种。

4.3.2 完整性

4.3.2.1 产品应提供确保应用程序或数据只有在被授权时才能被访问的手段。

注：一般情况下，产品应有基于角色的访问控制，在这样的机制当中，系统管理员级别的用户可对其他角色的用户进行可访问的授权，这样的授权功能允许每个用户只能访问被批准的应用程序或数据。

4.3.2.2 产品应提供适当的技术手段用于防止未授权用户登录。

注1：这样的技术手段可能包括：

——用户名口令；

——生物特征识别；

——USB 密钥设备；

——射频身份识别卡。

注2：注 1 中用户名口令应允许用户设置高等级的口令和口令复杂度管理。用户可以根据医疗器械的使用需求和安全需求来决定口令管理策略，产品应支持一种或多种口令策略的配置方式，至少应允许管理员配置口令复杂度要求和口令过期时间。

4.3.2.3 产品应提供用户会话在预设的无操作时间之后自动锁定或注销的手段，被授权的管理员应能对这个时间进行设置。产品也应提供手动锁定的手段。

4.3.3 可得性

4.3.3.1 产品应确保授权用户能够正常的访问数据。

4.3.3.2 若产品能够进行健康数据的本地存储，应提供手段以使得系统软件故障恢复后发生故障前存储的健康数据可获得，并应提供健康数据的备份和/或归档、恢复的手段。

4.3.3.3 如适用，制造商应在随机文件中规定推荐的健康数据备份和/或归档的方法和周期。

注：归档可以通过将健康数据存储在非易失性介质或经由网络传输至数据归档系统来完成。

4.3.3.4 在紧急情况下，用户应能通过紧急访问直接完成产品的预期医疗用途，而无需进行身份验证。

注：这种紧急访问的行为应能被检测和记录，这种记录应符合审计控制（参见 4.4.4.3）的要求。

4.3.4 审计

4.3.4.1 抗抵赖性

产品应提供实现有关于健康数据操作的抗抵赖性的手段。

4.3.4.2 可核查性

健康数据应有唯一的标识，用于追溯数据的来源。

4.3.4.3 审计控制

产品应能够通过在设备上创建审计跟踪来记录和检查用户的行为。审计记录不应被修改或删除。若审计记录包含保密数据，则应保证审计记录的安全，只有授权用户才可以访问。

需要追踪的行为至少应包括：

——身份认证；

——健康数据的查询、增加、删除、修改；

——健康数据的本地导入、导出；

——通过网络的健康数据的发送或接收；

——紧急访问。

每个行为应至少包括的属性有日期、时间、用户、事件、事件是否成功。

4.3.5 其他附加要求

4.3.5.1 物理防护

若产品有健康数据的存储功能，则应提供一种物理防护措施，防止对健康数据未经授权的访问。

4.3.5.2 系统加固

如提供工作站，制造商应对产品实施系统加固，以保证预期用途的前提下，保证安全性的最大化，来防止非授权用户获得系统控制权限或敏感信息。如不提供工作站，应提供系统加固措施或建议。

加固方式至少应包括：

——防火墙设置；

——端口关闭；

——服务禁用；

——快捷键封闭；

——操作系统、应用软件漏洞补丁安装。

注：敏感信息指健康数据以及系统、软件、密码/口令等信息。

4.3.5.3 安全指导

制造商应在随机文件中至少给出附录B中要求的产品安全能力以及各用户角色在安全方面职责的声明内容。

4.4 维护性

如制造商对产品提供安装或升级产品安全补丁的服务（包括OTS软件、自有软件），则应在随机文件中陈述和产品发布计划相应的维护服务。

4.5 可移植性

4.5.1 如果用户能够实施安装或卸载产品，制造商应在随机文件中规定安装或卸载的方式，且应能按此方式正确的实施安装或卸载。

4.5.2 对于制造商声明的所有支持的系统配置，软件应用程序应能成功安装和正确运行。

5 试验方法

5.1 兼容性

5.1.1 DICOM 符合性

通过以下两种方式的一种来验证是否符合要求。

方法一：基于附录C的测试规范，通过对制造商提供的DICOM符合性声明中所陈述的内容与产品进行验证，其结果应是正确的，且与产品实现一致。

方法二：制造商提供DICOM符合性测试对应的测试文档集，其中至少包括测试计划、测试用例、测试报告、测试工具的确认报告。DICOM符合性声明的内容应与测试文档集一致，DICOM符合性声明支持的特性应当由相应的测试报告予以支持。

注：DICOM标准本身并未指定一套测试工具，也没有提供指导制造商或第三方测试机构的测试过程方法，但制造商有责任对产品的DICOM符合性进行验证。因此，本标准提供了被广泛认可的DICOM符合性测试工具的基本要求，测试使用的测试工具的基本要求见附录D。

5.1.2 安全软件

通过实际测试和检查文档来检验是否符合要求,见附录C。

5.2 可靠性

通过实际测试和检查文档来检验是否符合要求，见附录C。

5.3 网络安全

5.3.1 保密性

通过实际测试和检查文档来检验是否符合要求，见附录C。

5.3.2 完整性

通过实际测试来检验是否符合要求，见附录C。

5.3.3 可得性

通过实际测试和检查文档来检验是否符合要求，见附录C。

5.3.4 审计

通过检查来检验是否符合要求，见附录C。

5.3.5 其他附加要求

5.3.5.1 物理防护

通过检查来检验是否符合要求，见附录C。

5.3.5.2 系统加固

通过检查来检验是否符合要求，见附录C。

5.3.5.3

通过检查文档来检验是否符合要求，见附录C。

5.4 维护性

通过检查文档来检验是否符合要求，见附录C。

5.5 可移植性

通过实际测试和检查文档来检验是否符合要求，见附录C。

附 录 A
（资料性附录）
DICOM 标准内容概述

A.1 文档结构

DICOM标准由以下部分组成：

- PS 3.1: 介绍和概述（类似于 A.1）；
- PS 3.2: 符合性；
- PS 3.3: 信息对象定义；
- PS 3.4: 服务类规范；
- PS 3.5: 数据结构和编码；
- PS 3.6: 数据字典；
- PS 3.7: 消息交换；
- PS 3.8: 支持消息交换的网络通信；
- PS 3.9: 失效；
- PS 3.10: 媒介交换的介质存储和文件格式；
- PS 3.11: 媒介存储应用程序配置文件；
- PS 3.12: 格式和物理媒介；
- PS 3.13: 失效；
- PS 3.14: 灰度标准显示功能；
- PS 3.15: 安全和系统管理配置文件；
- PS 3.16: 内容映射资源；
- PS 3.17: 解释性信息；
- PS 3.18: Web 服务；
- PS 3.19: 应用程序托管；
- PS 3.20：使用 HL7 临床文档体系结构的影像报告

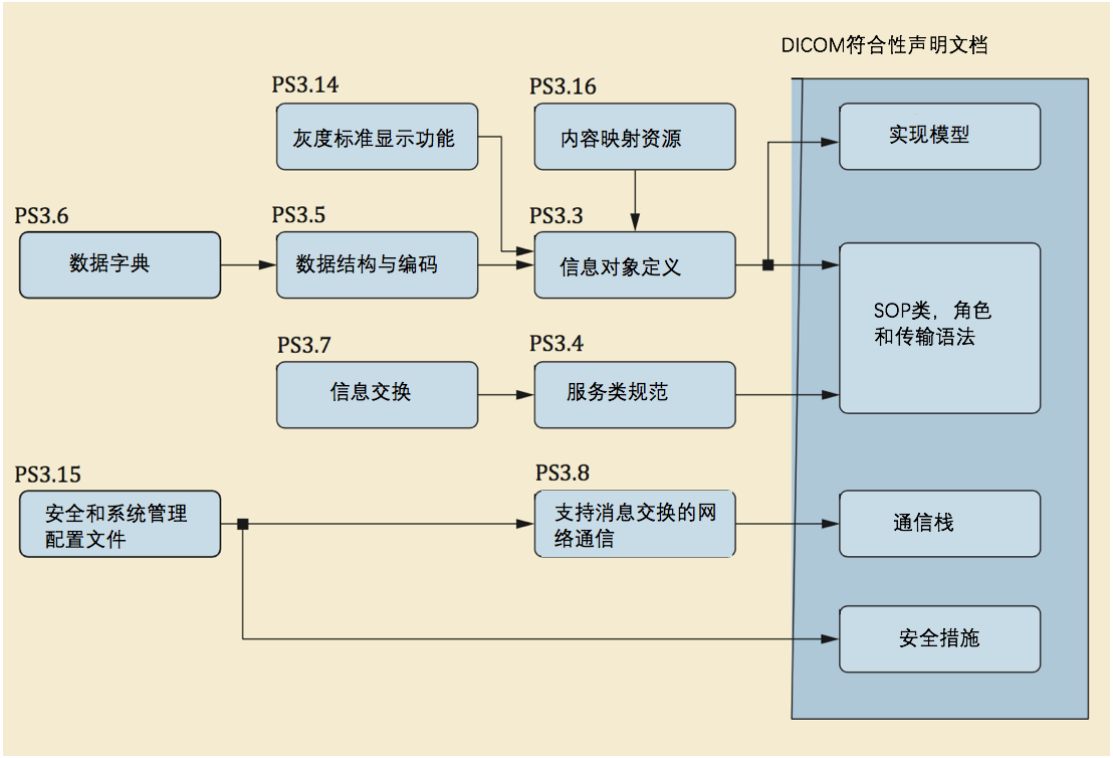
DICOM标准的这些部分是相关但独立的文件。 本节提供了每个部分的简要说明。

A.2 PS 3.2：符合性

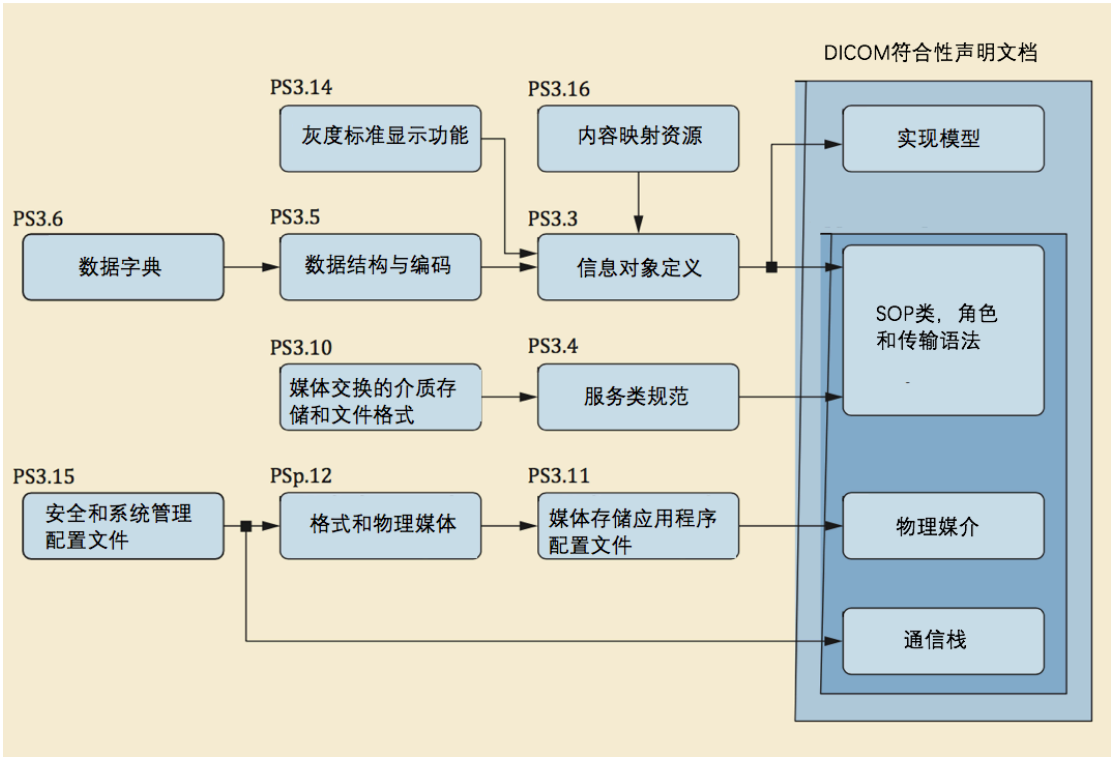
DICOM标准的PS 3.2定义了声明符合该标准的实现的原则。

- 符合性要求：PS 3.2 规定了任何要求符合性的实施应满足的一般要求。 它引用了标准其他部分的符合性部分。
- 符合性声明：PS 3.2 定义了符合性声明的结构。 它规定了应在符合性声明中出现的信息。它引用了标准其他部分的符合性声明部分。
- PS 3.2 没有指定测试/验证程序来评估实施是否符合标准。
- 图 A.1 和图 A.2 描绘了网络通信和媒介交换的符合性声明的构建过程。 符合性声明由以下部分组成：
- 该实现认可的集合的信息对象；
- 该实现支持的服务类集合；

- 该实现支持的通信协议或物理介质的集合；
- 该实现支持的一组安全措施。



图A.1　网络符合性声明的构建过程



图A.2　媒介符合性声明的构建过程

A.3　PS 3.3：信息对象定义

DICOM标准的PS 3.3规定了许多信息对象类，它们提供了适用于数字医学图像和相关信息的通信的真实世界实体的抽象定义（例如，波形，结构化报告，放射治疗剂量等）。 每个信息对象类定义包括其目的的描述和定义它的属性。 信息对象类不包括构成其定义的属性的值。

定义了两种类型的信息对象类：规范化和复合。

规范化信息对象类仅包括在所表示的真实世界实体中固有的那些属性。 例如，定义为归一化的研究信息对象类包含研究日期和研究时间属性，因为它们在实际研究中是固有的。 然而，患者名称不是研究信息对象类的属性，因为它是在执行研究的患者中固有的，而不是研究本身。

复合信息对象类可以另外包括与现实世界实体相关但不固有的属性。例如，计算机断层扫描图像信息对象类，它被定义为是复合的，包含两个属性，一是图像固有的属性（如图像日期），二是与图像相关但非固有的属性（如病人的名字）。复合信息对象类提供了一个结构化的框架，用于表达图像数据和相关数据需要密切相关的图像的通信要求。

为了简化信息对象类定义，将每个信息对象类的属性分区，并将类似的属性进行分组。这些属性组被指定为独立模块，并可能被其他复合信息对象类重新使用。

PS 3.3定义了真实世界的模型以及相应的信息模型，该模型反映在信息对象定义中。本标准之后的版本会扩展这组信息对象以支持新功能。

为了表示真实世界实体的发生，创建了一个信息对象实例，该实例包含了信息对象类的属性值。此信息对象实例的属性值可能随时间变化，以准确反映其所代表的实体的变化状态。这是通过在信息对象实例上执行不同的基本操作来呈现定义为服务类的特定服务集的。这些服务类定义在PS 3.4的标准中。

A.4　PS 3.4：服务类规范

DICOM标准的PS 3.4部分定义了一系列服务类。服务类将一个或多个信息对象与一个或多个命令关联在这些对象上执行。服务类规范对命令元素的状态要求以及如何将生成的命令应用于信息对象。通信服务提供商和用户的服务类规范的状态要求。

DICOM标准的PS 3.4部分定义了所有服务类共有的特点，以及如何构造针对个人服务类的符合性声明。它包含了许多描述个人服务类的规范性附录。

服务类的示例包括：

1）存储服务类;

2）查询/检索服务类;

3）基本工作列表管理服务类;

4）打印管理服务类。

PS 3.4定义了对PS 3.3中定义的信息对象执行的操作。 PS 3.7定义了使用这些命令完成PS 3.4中描述的操作和通知的命令和协议。

A.5　PS 3.5：数据结构和语义

DICOM标准的PS 3.5规定了DICOM应用程序如何构造和编码由使用DICOM标准的PS 3.3和PS 3.4中定义的信息对象和服务类所产生的数据集信息。 规定了许多标准图像压缩技术（例如，JPEG无损和有损）的支持。

PS 3.5强调了在构造消息传送中数据流所必需的编码规则，如DICOM标准的PS 3.7中所规定的。 此数据流由构成数据集的数据元素集合生成。

PS 3.5还定义了许多信息对象共有的多个通用函数的语义。 PS 3.5定义了DICOM中使用的国际字符集的编码规则。

A.6 PS 3.6：数据字典

DICOM标准的PS 3.6是集中式注册表，其定义可用于表示信息的所有DICOM数据元素的集合，以及用于表示可交换媒介编码的元素和由DICOM分配的唯一标识项目的列表。

对于每个元素，PS 3.6指定：

- 唯一标签，由组和元素号组成；
- 名称；
- 值表示（字符串，整数等）；
- 值的多重性（每个属性有多少个值）；
- 是否失效。

对于每个唯一标识的项目，PS 3.6指定：

- 唯一值，其为具有由小数点分隔且限于 64 个字符的多个组件的数字；
- 名称；
- 类型，信息对象类，用于数据传输的编码的定义或某些公知的信息对象实例；
- 其中定义了 DICOM 标准的一部分。

A.7 PS 3.7：消息交换

DICOM标准的PS 3.7规定了医疗成像环境中应用程序使用的服务和协议，以通过PS 3.8中定义的通信支持服务交换消息。 消息由PS 3.7中定义的命令流和PS 3.5中定义的可选数据流组成。

PS 3.7规定：

- 对 PS 3.4 中定义的服务类提供的操作和通知（DIMSE 服务）；
- 建立和终止由 PS 3.8 中规定的通信支持的协会的规则，以及对未完成交易的影响;
- 管理命令请求和响应的交换的规则；
- 编译命令流和消息所必需的编码规则。

A.8 PS 3.8：网络通信支持消息交换

DICOM标准的PS 3.8规定了通信服务的必要支持和上层协议，在网络环境下，应用程序之间的通信为DICOM标准PS 3.3，PS 3.4，PS 3.5，PS 3.6和PS 3.7。这些通信服务和协议确保DICOM应用之间的通信能够在网络间以一种有效且协调的方式进行。

在PS 3.8指定的通信服务是由OSI表示服务提供的服务的一个真子集（ISO/IEC 8822）以及OSI关联控制服务单元（ACSE）（ISO/IEC 8649）的一个真子集。它们被称为上层服务，它允许同等的应用程序建立关联、传递消息和终止关联。

上层服务这一定义指定DICOM上层协议与TCP/IP传输协议一起使用。

PS 3.8指定的TCP/IP通信协议是一个通用的通信协议而非特定的DICOM标准。图3显示了这个协议栈。

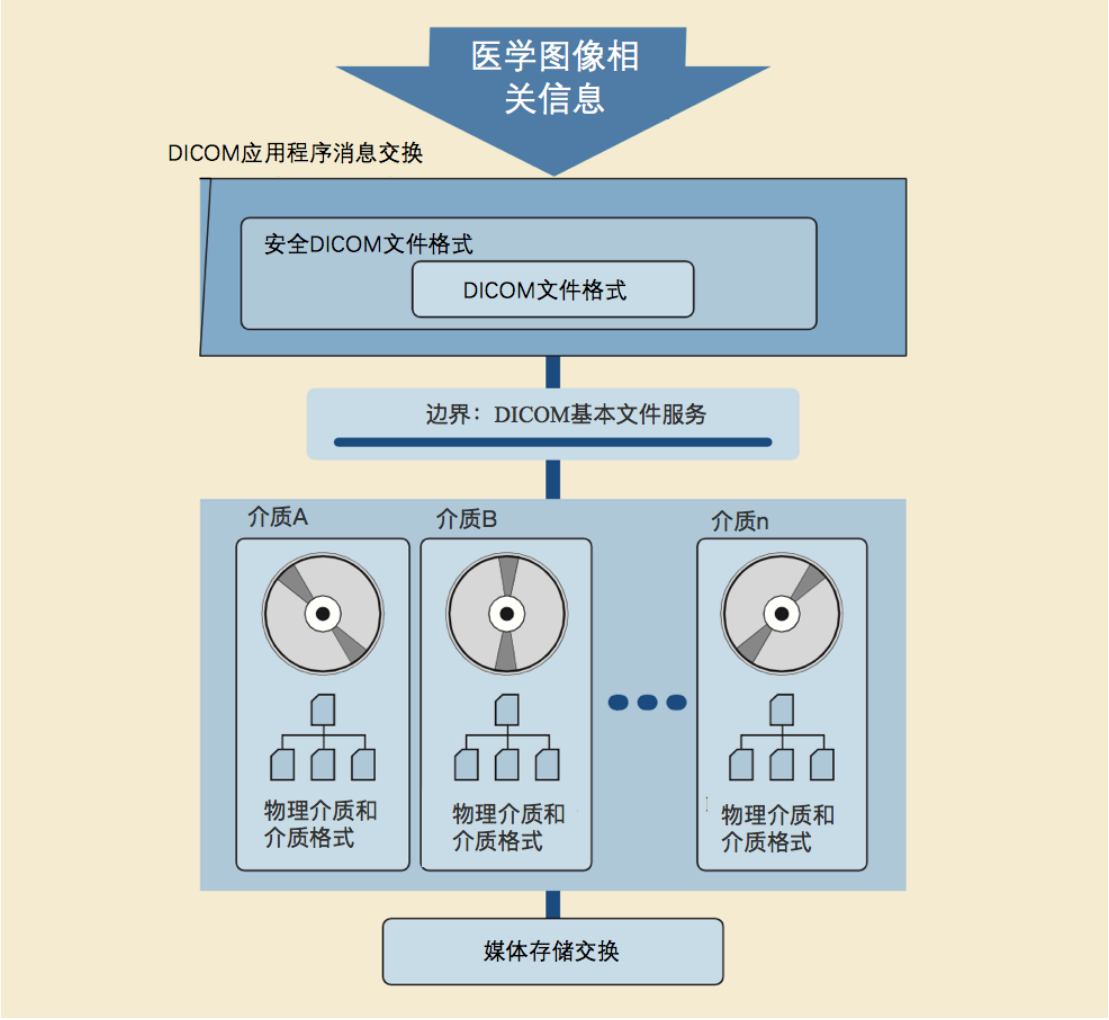
A.9 PS 3.9：失效（以前的点对点通信支持消息交换）

DICOM标准的PS 3.9先前以与ACR-NEMA 2.0兼容的方式指定了用于点对点通信的服务和协议。 它已经失效了。

A.10 PS 3.10 媒介存储和文件格式

DICOM标准的PS 3.10规定了在可移动介质上存储医学成像信息的一般模型（见图A.3）。 本部分的目的是提供允许在广泛的物理存储介质上交换各种类型的医学图像和相关信息的框架。

参见图A.3，DICOM媒介通信模式。



图A.3 DICOM 媒介通信模式

PS 3.10规定：

用于在存储介质上存储医学图像和相关信息的分层模型;该模型引入了媒介存储应用框架文件的概念，其指定了媒介存储实现可以声明符合性的DICOM标准的特定应用的子集;

注意，这种符合性仅适用于存储介质内容的写入，读取和更新。

持任何信息对象的封装的DICOM文件格式;

支持在加密包络中封装DICOM文件格式的安全DICOM文件格式;

提供与底层媒介格式和物理媒介无关的DICOM文件服务。

PS 3.10定义了各种媒介存储概念：

a）在单个介质上识别文件集合的方法；

b）在特定文件系统中命名DICOM文件的方法。

A.11 PS 3.11：媒介存储应用程序配置文件

DICOM标准的PS 3.11规定了DICOM标准的应用特定子集，其实现可以声明符合性。 这些应用程序特定子集在本子条款中称为应用框架规范。 这种符合性声明适用于医疗图像和用于特定临床使用的存储介质上的相关信息的互操作交换。 它遵循PS 3.10中定义的框架，用于在存储介质上交换各种类型的信息。

应用框架规范附录包括以下主要部分：

1） 应用框架规范的名称或分组在相关类中的应用框架规范列表；

2） 对应用框架规范的临床内容的描述；

3） 具有应用框架规范和相关选项的设备角色的媒介存储服务类的定义；

4） 描述应用框架规范的操作要求的信息部分；

5） 支持的信息对象类和相关联的信息对象的规范以及要用于数据传输的编码；

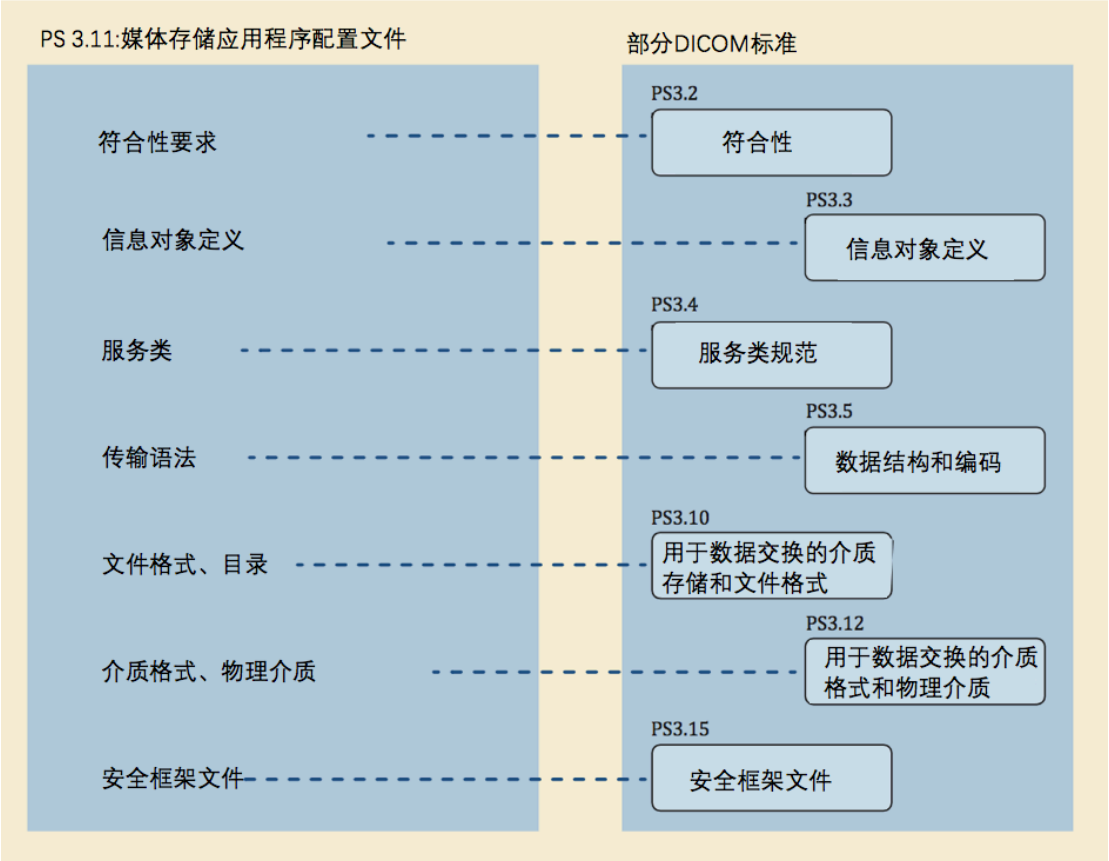
6） 选择要使用的媒介格式和物理媒介；

7） 需要指定的其他参数以确保可互操作的媒介交换；

8） 用于选择与安全媒介存储应用框架规范一起使用的加密技术的安全参数。

DICOM标准的结构和应用框架规范的机制对于附加的信息对象类是一种扩展，且新的交换介质是直接的。

图A.4显示了应用框架规范的各个方面如何映射到DICOM标准的各个部分。



图A.4　应用框架文件和DICOM的部分之间的关系

A.12　PS 3.12：数据交换的存储功能和媒介格式

DICOM标准的这一部分便于在医疗环境中的应用之间交换信息，具体规定：
用于描述媒介存储模型与特定物理媒介和媒介格式之间的关系的结构;
特定物理媒介特性和相关媒介格式。

A.13　PS 3.13：失效（以前的打印管理点对点通信支持）

PS 3.13先前规定了用于打印管理服务的点对点通信的服务和协议;它已经失效了。

A.14　PS 3.14：灰度标准显示功能

PS 3.14规定了用于一致显示灰度图像的标准化显示功能。该功能提供了用于校准特定显示系统的方法，用于在不同的显示介质（例如，监视器和打印机）上一致地呈现图像的目的。

所选择的显示功能基于人的视觉感知。人眼对比敏感度在显示装置的亮度范围内是明显非线性的。该DICOM标准使用Barten的人类视觉系统模型。

A.15　PS 3.15：安全和系统管理配置文件

DICOM标准的PS 3.15规定了实现可以声明符合性的安全和系统管理框架文件。安全和系统管理框架文件通过引用外部开发的标准协议（如DHCP，LDAP，TLS和ISCL）来定义。安全协议可以使用诸如公钥和“智能卡”的安全技术。 数据加密可以使用各种标准化数据加密方案。

本部分不涉及安全策略的问题。该DICOM标准仅提供可用于实现关于DICOM对象的交换的安全策略的机制。 建立适当的安全策略是本地管理员的责任。

A.16 PS 3.16：内容映射资源

DICOM标准的PS 3.16规定：

- 用于将文档结构化为 DICOM 信息对象的模板;
- 用于信息对象的编码项集合;
- 由 DICOM 定义和维护的术语词典;
- 编码术语的国家特定翻译。

A.17 PS 3.17：说明信息

DICOM 标准的 PS3.17 提供含有信息性以及规范性附录和解释信息。

A.18 PS 3.18：Web服务

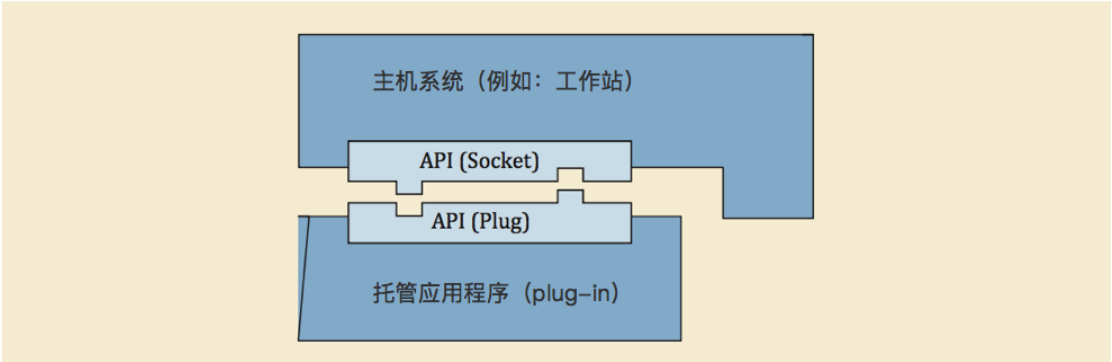
DICOM标准的PS3.18规定了Web服务可用于检索或存储DICOM对象的方法。

检索数据的请求指定了响应主体的媒介类型（格式）。 存储数据的请求指定请求主体的媒介类型。

在PS3.18中定义的HTTP请求足以使HTTP服务器充当DICOM SCU（服务类用户），以使用基本的DICOM功能从相应的DICOM SCP（服务类提供者）检索或存储所请求的对象，如 PS3.4和PS3.7，也就是说HTTP服务器可以作为DICOM SCP的代理。

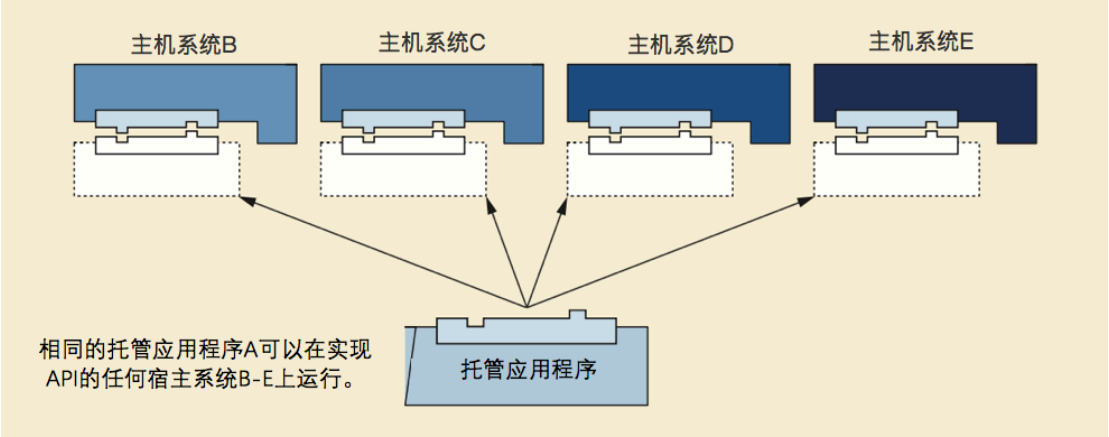
A.19 PS3.19: 应用程序托管

DICOM标准的PS3.19为基于DICOM的医疗计算系统指定了一个应用程序编程接口（API），写入该标准化接口的程序可以“插入”程序（见图A.5）。 托管系统实施者只需要创建一次标准化的API来支持各种附加的托管应用程序。



图A.5 托管应用程序和托管系统之间的接口

在传统的“插件”模型中，“插件”专用于特定的主机系统（例如网页浏览程序），并且可能不在其他主机系统（例如其他网页浏览程序）下运行。PS3.19定义了一个可以被任何主机系统实现的API。 写入API的“插件”托管应用程序可以在任何由实现该API的托管系统提供的环境中运行（参见图A.6）。



图A.6　通过托管应用程序的平台独立性

PS3.19指定了托管系统和托管应用程序之间的交互和应用程序编程接口（API）。 PS3.19还定义了API使用的数据模型。

A.20　PS3.20：使用HL7 临床文件架构的影像报告

DICOM标准PS3.20规定了使用HL7临床文件结构第2版（CDA R2或简称CDA）标准编码成像报告的模板。在这个范围内是使用用于筛选，诊断或治疗目的的成像的专业的临床程序报告。

PS3.20构成了CDA的实施指南，并与HL7开发的CDA实施指南的标准化模板的方法相一致。它还提供用户链接数据的数据元素的商业名称，例如， 由报告创作应用程序收集到特定的CDA编码元素。

作为成像报告的实施指南，特别关注在成像过程中收集的数据作为报告中的明确证据。这些数据包括图像，波形，测量结果，注释以及以DICOM SOP实例管理的其他分析结果。 具体而言，PS3.20包含一个转换为DICOM结构化报告实例的CDA文档的规范，这些实例代表成像报告。

附 录 B
（规范性附录）
产品安全能力声明模板

B.1 产品网络安全能力声明模板

产品网络安全能力声明模板见表B.1。

表B.1 产品安全能力声明模板

<table>
<tr><td colspan="4">设备描述</td></tr>
<tr><td>设备名称：</td><td>型号：</td><td>厂商：</td><td>类型：</td></tr>
<tr><td>软件版本：</td><td>软件发布日期：</td><td>文档编号：</td><td>文档发布日期：</td></tr>
<tr><td rowspan="2">厂商或代理商联系信息</td><td>厂商名称：</td><td colspan="2" rowspan="2">厂商联系方式：</td></tr>
<tr><td>代理商名称：</td></tr>
<tr><td colspan="4">设备在网络中的预期用途：</td></tr>
<tr><td colspan="4">网络安全能力声明</td></tr>
<tr><td colspan="2">保密性（4.3.1）声明</td><td>声明结果
（是/否）</td><td>备注</td></tr>
<tr><td colspan="2">1 设备是否存储隐私数据？</td><td></td><td></td></tr>
<tr><td colspan="2">2 设备所存储的隐私数据是否包括：</td><td></td><td></td></tr>
<tr><td colspan="2">2.1 个人数据（例如，姓名、住址、身份证号码、医疗卡号码等）</td><td></td><td></td></tr>
<tr><td colspan="2">2.2 医学记录（例如，医学记录，账户，诊断/治疗日期等）</td><td></td><td></td></tr>
<tr><td colspan="2">2.3 诊断数据（例如，医学影像，测试结果等）</td><td></td><td></td></tr>
<tr><td colspan="2">2.4 由设备使用者/操作者输入的非结构化文本</td><td></td><td></td></tr>
<tr><td colspan="2">2.5 生物识别数据</td><td></td><td></td></tr>
<tr><td colspan="2">2.6 个人财务数据</td><td></td><td></td></tr>
<tr><td colspan="2">3 设备是否采用以下机制保证隐私数据存储保密性：</td><td></td><td></td></tr>
<tr><td colspan="2">3.1 数据加密或信息隐藏</td><td></td><td></td></tr>
<tr><td colspan="2">4 设备是否采用以下机制保证健康数据传输保密性：</td><td></td><td></td></tr>
<tr><td colspan="2">4.1 节点认证或白名单</td><td></td><td></td></tr>
<tr><td colspan="2">4.2 加密通信协议</td><td></td><td></td></tr>
<tr><td colspan="2">5 是否提供健康数据导出时保护患者隐私性的手段？</td><td></td><td></td></tr>
<tr><td colspan="4">备注详细说明：</td></tr>
</table>

完整性（4.3.2）声明	声明结果（是/否）	备注
1 设备是否使用一定的访问控制技术以防止未授权访问？		
2 设备是否采用以下身份认证技术：		
2.1 用户名口令		
2.2 生物特征识别		
2.3 USB密钥设备		
2.4 射频身份识别卡		
3 设备能否在一定的无活动时间后自动锁定？		
3.1 设备是否提供设置自动锁定的时间的功能？		
3.2 设备是否提供手动锁定的功能？		
备注详细说明：		
可得性（4.3.3）声明	声明结果（是/否）	备注
1 是否提供确保授权用户能够正常的访问数据？		
2 是否提供健康数据的备份和恢复的手段？		
2.1是否在随机文档中陈述健康数据备份的方法和周期？		
3 是否能够紧急访问？		
备注详细说明：		
审计（4.3.4）声明条	声明结果（是/否）	备注
1 是否提供健康数据操作抗抵赖性的手段？		
2 是否对健康数据进行唯一标识？		
2.1是否提供基于唯一标识的溯源手段？		
3 是否对用户行为进行审计，并生成审计记录？		
3.1审计追踪是否包括以下行为：		
3.1.1 身份认证；		
3.1.2 健康数据的查询、增加、删除、修改；		
3.1.3 健康数据的本地导入、导出；		
3.1.4 通过网络的健康数据的发送或接收。		
3.1.5 紧急访问		
3.2 审计追踪的行为是否包括以下属性：		
3.2.1 日期；		
3.2.2 时间；		
3.2.3 用户；		
3.2.4 事件；		
3.2.5 事件是否成功。		
3.3设备是否提供保证审计追踪记录保密性的机制（例如数据加密、访问控制等）？		

备注详细说明：		
其他附加要求（4.3.5）		
声明条目	声明结果 （是/否）	备注
1 是否提供用于保护数据安全的物理防护措施？		
2 是否提供以下系统加固手段：		
防火墙设置；		
端口关闭；		
服务禁用；		
快捷键封闭。		
备注详细说明：		

附 录 C
（规范性附录）
测试规范

C.1 概述

本测试规范测试目的是证实产品是否符合第4章的要求，产品测试应基于软件工程测试的要求进行。按照此测试规范编制的文档一般应包含测试计划、测试用例和测试结果（报告），但本规范并不对具体有哪些文档做出规定。这些文档不应与产品矛盾，如果有多个文档构成，那么每个文档之间也不应自相矛盾。

注：本测试规范参考了GB/T 25000.51-2016的第六章的要求，编制相关文档时可参考上述标准中的对应条款。

C.2 测试用例的说明

对每个测试用例的说明应包括：

a) 测试目标；
b) 唯一性标识符；
c) 测试的输入数据和测试边界；
d) 详细实施步骤；
e) 系统的预期行为；
f) 测试用例的预期输出；
g) 结果解释的准则；
h) 用于判定测试用例的肯定或否定结果的准则。

注1：编制的测试用例应基于一定的测试规程来进行测试。

注2：本标准不提供测试用例模板，也不对测试用例的模板进行要求，模板请参考 GB/T 15532-2008。

C.3 测试用例应考虑的内容

创建测试用例时，应至少给出考虑的建议和其通过/失败准则如表C.1所示；但在表C.1中，并没有列出通过查验文档的方式来验证其符合性的条款。

表C.1 测试用例应考虑的内容

条款	测试用例编制应考虑的内容	通过/失败准则
4.1.1 DICOM 符合性	见5.1.1试验方法	通过5.1.1试验方法的方式判定是否符合4.1.1
4.1.2 安全软件	考虑制造商规定与之兼容的安全软件是否兼容	配置规定的安全软件应不影响产品的正常使用
4.2.1 容错性	考虑可能出现的网络异常的情况，如从系统断开网络连接、拔掉网线	数据不应丢失
	考虑可能出现的失去电源的情况，如直接关机、	数据不应丢失。

	直接断开电源	
	考虑可能导致传输中断的使用者错误的操作	数据不应丢失。
	考虑可能出现应用程序自身逻辑出错的场景，如应用程序宕机。	数据不应丢失。
	考虑模拟一种数据被篡改的场景	应用程序不应崩溃
4.2.2 易恢复性	考虑模拟可能出现的典型的网络响应时间超时的场景，通过失败准则宜根据实际的产品及应用场景考虑时间的长短。	应提示最终用户超时。
4.2.3 数据丢失的防止	考虑可能出现的系统存储容量达到制造商规定的容量的上限时，进行继续进行数据存储行为	产品应有相应的机制来控制非预期的数据丢失，且提示用户容量状况，宜禁止继续存入图像。
	考虑可能出现的系统存储容量即将达到制造商规定的容量的上限时，进行继续进行数据存储行为	产品应有相应的机制来控制非预期的数据丢失，且提示用户容量状况，宜禁止继续存入图像。
	考虑可能出现的最终用户非预期输入导致的数据丢失的情况	数据不应丢失。
4.3.1 保密性		
4.3.1.1 存储保密性	考虑可能出现的非授权访问加密数据的情况	健康数据的明文隐私信息不能被获取。
4.3.1.2 传输保密性	如适用，检查产品是否使用使用节点认证或白名单的方式	功能正确实现。
	如适用，考虑产品是否能与未经节点认证或白名单外的节点通信	非法通信不能被建立。
	如适用，考虑未经节点认证或白名单外的节点是否能与产品建立通信	非法通信不能被建立。
	考虑通过网络嗅探的方式捕捉健康数据的情况	健康数据的明文隐私信息不能被获取。
	考虑攻击者通过建立远程网络连接窃取健康数据的情况	健康数据的明文隐私信息不能被获取。
4.3.1.3 患者隐私的保护	如适用，以匿名化的形式导出健康数据，考虑是否能在未经认证的情况下查看或以明文形式获得患者隐私数据	4.3.1.3规定的患者信息不能被查看。
4.3.2 完整性		
4.3.2.1	考虑产品是否提供确保应用程序或数据只有在被授权时才能被访问的手段	功能正确实现。
4.3.2.2	考虑产品是否提供适当的技术手段用于防止未授权用户登录	功能正确实现。
4.3.2.3	考虑产品是否提供了用户会话在预设的无操作时间之后自动锁定或注销的手段	功能正确实现。
	考虑产品是否能够令被授权的管理员对上述时间进行设置	功能正确实现。
	考虑产品是否提供手动锁定的手段	功能正确实现。

	考虑数据完整性被破坏的情况，例如，未授权登录或在管理员离开未锁定/注销等前提下，攻击者可以修改数据的情况	健康数据的完整性不应被破坏。
4.3.3 可得性		
4.3.3.1	在正常的情况下，检查产品是否能够确保授权用户能够正常的访问数据	功能正确实现。
4.3.3.2	如适用，考虑在系统遭受攻击、宕机、导致数据丢失的情况	健康数据应定期备份并可恢复，保证授权用户可正常访问。
4.3.3.4	考虑管理员/操作员不在的情况，能够继续提供服务；考虑用户不会操作紧急访问的问题	产品应提供权限受限的紧急访问功能；产品应在随机文档中提供紧急访问操作的描述。
4.3.4.1 抗抵赖性	考虑针对健康数据操作的抵赖情况	应提供抗抵赖的手段，例如访问控制的角色、健康数据签名、时间戳等。
4.3.4.2 可核查性	考虑需要健康数据溯源的情况	健康数据应提供至少一种唯一标识，用于溯源。
4.3.4.3 审计控制	考虑需要审计用户行为的情况;考虑审计日志被窃取、嗅探、修改的情况	审计日志中应追踪4.3.4.3要求的行为;审计日志不能被修改或删除。
4.3.5.1 物理防护	考虑硬盘被盗窃的情况	除非用工具否则不能拆卸
4.3.5.2 系统加固	如适用，检查产品是否按照4.3.5.2的要求进行了系统加固，例如配置防火墙、端口关闭、快捷键移除等	功能正确实现。
4.5 可移植性		
4.5.1	如适用，检查产品是否能够按照制造商规定的方式安装产品（软件）	功能正确实现。
	如适用，检查产品是否能够按照制造商规定的方式卸载产品（软件）	功能正确实现。
4.5.2	检查产品是否能够支持制造商声明的所有支持的系统配置	功能正确实现。

注：4.3.3.3、4.3.5.3、4.4通过查验文档的方式来验证其符合性。

附 录 D
（规范性附录）
设备连通性符合性测试工具基本要求

D.1 设备连通性符合性测试工具基本要求

当要符合本标准4.1.1条款时，可能用到5.1.1条款中提到的测试工具，测试工具应满足以下要求：

a) 测试工具需独立于指定的测试环境或测试用例，对被测内容不能有依赖关系。
b) 能够配置其 DICOM 节点属性（包括，AE 标题、端口、PDU 属性等内容），完成与被测 DICOM 节点的连接。
c) 能够扮演 SCP 与 SCU 的角色，能够生成/发送并接受/验证指定的 DICOM 编码信息，并能够精确定义各级 DICOM 消息或信息内容，从而精确定义传输过程。
d) 能够进行简单的逻辑判断以完成某些需要验证或判断的传输过程。
e) 能够提供清晰的输出，能够浏览传输过程中各级 DICOM 消息或信息内容。
f) 接收的影像数据内容可用 DICOM 或数据集格式存储，便于浏览及验证。

附 录 E
（资料性附录）
部分条款说明

E.1 4.1.2 条款说明

在一些实际情况当中，普通用户无法对安全软件和应用程序的兼容性进行评估，因此对于制造商来说，有责任对与那些安全软件进行兼容作出规定以防安全软件在用户不知情的情况下失效。但本标准并不会对安装何种、哪些安全软件作出规定。

E.2 4.2.3 条款说明

第三列项：如果授权的用户做出数据删除动作，对于本标准来说不认为是一种非预期输入。

E.3 4.3.1.1 条款说明

对于本标准来说，认为数据加密是对数据文件内容的加密。对于将明文数据文件存储在数据库当中，而对数据库做了未授权访问防止机制的方式，不认为是一种数据加密，但可以认为是一种保证数据完整性的手段。制造商仅有责任提供这种加密手段，但加密手段使用与否应由用户（医疗机构）决定。

E.4 4.3.1.2 条款说明

对于本标准来说，这种保密性的手段可能包括了：提供虚拟专用网络（VPN）加密信道、使用HTTPS协议（基于SSL的HTTP协议）等手段，但本标准并不限制传输的加密方式。此外，当用于远程诊断，或者类似的医疗用途之时，健康数据需要在公共网络中传输时，健康数据将会暴露在公共网络之中，这种情况被广泛认为是不安全的，在这种情况下的传输保密性则显得尤为重要。

E.5 4.3.2.1 条款说明

对于这样的基于角色的访问控制，一般情况下，制造商在缺省条件宜配置以下角色：服务工程师、管理员、操作者。而每个角色应该有不同的权限，但本标准中并不会限定角色的种类和角色种类的数量。

E.6 4.3.2.2 条款说明

用户名口令的复杂度通常由使用者根据临床使用需求来设定，但同时产品应支持使用者设置口令复杂度高的密码。口令复杂度密码管理可使用以下几种方式：1)支持统一的管理；2)可配置的本地配置规则；3）默认的本地配置规则。口令复杂度高的密码这里指：应支持设置不小于位

E.7 4.3.2.4 条款说明

在大多数场景下，最终用户（操作者）可能会离开设备一段时间，在这段时间内，可能会发生未授权的用户对程序或系统进行访问而不需要身份验证的情况，这样的情况在一些临床应用的场景下是危险的，尤其是那些辐射剂量较大的诊断场景。此外，这段时间也有可能未授权的用户窃取或破坏健康数据。因此，管理员在设置时间时，应考虑这些临床应用场景。

但在另外一些临床应用中，最终用户（操作者）对应用程序的需求可能只是查看应用程序提供的影像数据而并非经常会去操作应用程序，类似于这样的场景下，则应当关闭自动锁定或注销的功能，否则可能会严重影响产品的易用性和可用性。

E.8　4.3.4.1 条款说明

抗抵赖性可通过角色访问控制、健康数据的数字签名、时间戳等方式联合实现，但本标准并不限制实现抗抵赖性的方式。

E.9　4.3.4.3 条款说明

第五列项：作为本标准的建议，产品应有这样的能力：在紧急情况下，临床用户需要能够快速访问健康数据或使用产品的基本临床功能，而无需个人用户标识和身份验证。但是为了监控这样的功能的使用和防止这样的功能滥用，这样的行为应进行审计控制。

E.10　4.3.5.2 条款说明

系统加固被认为是在应用软件难以修改或者不方便修改的前提下提高整体安全性的最有效的手段。合理的安全加固能够消除系统上存在的已知漏洞，减小攻击接口，提升产品整体安全等级。软件漏洞发布网址可参考国家信息安全漏洞共享平台（www.cnvd.org.cn）或美国信息安全漏洞数据库（nvd.nist.gov）。