**辽宁省医学影像云技术规范**

**（征求意见稿）**

**辽宁省卫生健康委员会**

目 次

[1 范围 6](#_Toc97885892)

[2 规范性引用文件 6](#_Toc97885893)

[3 术语、定义和缩略语 7](#_Toc97885894)

[3.1 术语和定义 7](#_Toc97885895)

[3.1.1 医学影像云 7](#_Toc97885896)

[3.2 缩略语 7](#_Toc97885897)

[4 数据采集规范 8](#_Toc97885898)

[4.1 影像数据采集方式 8](#_Toc97885899)

[4.1.1 影像索引处理 8](#_Toc97885900)

[4.1.2 影像加密处理 8](#_Toc97885901)

[4.1.3 影像压缩处理 8](#_Toc97885902)

[4.1.4 影像交互 8](#_Toc97885903)

[4.2 结构化数据采集 8](#_Toc97885904)

[4.2.1 信息采集方式 8](#_Toc97885905)

[4.2.2 报告采集 8](#_Toc97885906)

[4.3 前置网关 9](#_Toc97885907)

[4.3.1 主要技术要求 9](#_Toc97885908)

[5 数据传输规范 10](#_Toc97885909)

[6 影像云平台技术规范 10](#_Toc97885910)

[6.1 数据内容 10](#_Toc97885911)

[6.1.1 主索引 10](#_Toc97885912)

[6.1.2 患者基本信息 10](#_Toc97885913)

[6.1.3 检查信息 10](#_Toc97885914)

[6.1.4 报告数据 10](#_Toc97885915)

[6.1.5 影像数据 10](#_Toc97885916)

[6.2 数据存储 11](#_Toc97885917)

[6.2.1 云计算要求 11](#_Toc97885918)

[6.2.2 云存储要求 11](#_Toc97885919)

[6.3 数据灾备 11](#_Toc97885920)

[7 影像云平台安全规范 11](#_Toc97885921)

[7.1 基本要求 11](#_Toc97885922)

[7.2 安全体系建设 11](#_Toc97885923)

[8 机房物理环境技术规范 12](#_Toc97885924)

**前 言**

本标准依据GB/T1.1-2020给出的规则起草。

本标准起草单位：辽宁省卫生信息学会、

**引 言**

为贯彻落实国家《医疗机构检查检验结果互认管理办法》，推动辽宁省医学影像检查数据互联互通、共享互认，助力优质医疗资源下沉的目标，借鉴国际和国内先进经验，结合辽宁省的实际发展情况，制定《辽宁省医学影像云技术规范》，促进辽宁省医学影像云平台建设、管理与运营。

本规范针对医学影像检查数据的采集、传输、存储、硬件资源及数据管理等各环节提出技术性基本要求。明确规范了影像云平台内的个人影像检查唯一主索引标识要求，明确影像检查省内跨医疗机构、跨平台的主索引要求，以实现全省影像检查数据互联互通、共享互认。并按照《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》规定，要求医学影像云所涉及的计算和存储资源应在本地（辽宁省内）实现，以确保数据安全可控、可追溯。

辽宁省医学影像云技术规范

# 范围

本规范规定了跨医疗机构的区域性影像云的数据采集、传输、存储以及安全等方面内容。

本规范不适用医疗机构或医疗集团内部影像系统，即PACS/RIS系统。

#  规范性引用文件

下列文件对于本规范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）适用于本规范。

GB 50348-2004《安全防范工程技术规范》

GB/T 22239-2008《信息系统安全等级保护基本要求》

GB/T 24856-2009《信息系统等级保护安全设计技术要求》

GB/T 31168-2014《信息安全技术云计算服务安全能力要求》

GB/T 31458-2015《医院安全技术防范系统要求》

GB/T 35279-2017《信息安全技术云计算安全参考架构》

GB/T 35273-2017《信息安全技术个人信息安全规范》

GB/T 51380-2019 宽带光纤接入工程技术标准

YD 5095-2014 同步数字体系（SDH）光纤传输系统工程设计规范

YD 5208-2014 光传送网(OTN)工程设计暂行规定

YD 1475-2006 接入网技术要求-基于以太网方式的无源光网络（EPON)

YD 5206-2014 宽带光纤接入工程设计规范

YDT 2274-2011 接入网技术要求-10Gbits以太网无源光网络 (10 GPEON)

GA38-2004《中华人民共和国公共安全行业标准》

GA 308-2001《安全防范系统验收规则》

GA/T 670-2006《安全防范系统雷电浪涌防护技术要求》

GB/T 25068《信息技术安全技术IT网络安全》

GB 50174-2017《电子信息系统机房设计规范》

GA/T 75-1994《安全防范工程程序与要求》

GA/T 1390.2-2017《信息安全技术 网络安全等级保护基本要求 第2部分：云计算安全扩展要求》

WS538—2017 医学数字影像通信基本数据集

ISO/IEC 11801《信息技术-用户基础设施结构化布线》

IEEE 802.3u《快速以太网100Base-TX标准》

# 术语、定义和缩略语

## 术语和定义

下列术语和定义适用于本文件。

### 医学影像云

以医学影像信息的云存储为数据基础，以医学影像云计算应用服务为核心，以虚拟化和大数据技术为支撑，通过云方式，覆盖区域内多级医疗机构，为患者、医疗机构等提供医学影像数据共享互认，进而实现云端影像、远程会诊、远程诊断等云服务模式。

## 缩略语

下列缩略语适用于本文件。

AES：高级加密标准算法 (Advanced Encryption Standard)

S3：简易储存服务（Simple Storage Service）

bzip2：压缩文件存档（Compressed file archive）

DICOM：医学数字影像与通信(Digital Imaging and Communications in Medicine)

HTTPS：超文本传输安全协议（Hyper Text Transfer Protocol over SecureSocket Layer）

OSS：对象存储 (Object Storage Service)

PACS：医学影像存储与传输系统 (Picture Archiving and Communication System)

RIS：放射科信息系统 (Radio Information System)

VPC：逻辑隔离网络（Virtual Private Cloud）

# 数据采集规范

## 影像数据采集方式

影像数据采集可采用前置或无前置两种模式。前置模式需要在医院部署独立数据采集设备，无前置模式需要把数据采集软件部署在医院服务器或工作站上，通过DICOM的C-STORE或C-MOVE协议的方式来获取影像。

### 影像信息处理

通过读取原始DICOM影像数据的TAG值，获得患者姓名、性别、检查编号等基础信息并进行记录管理。

### 影像加密处理

支持DICOM TLS加密方式，将DICOM影像文件在传输过程的相关信息进行加密。

### 影像压缩处理

对于诊断级数据，应采用DICOM无损压缩。对于浏览级数据，可采用其他有效压缩算法。

### 影像交互

将DICOM基础信息及的DICOM影像实体文件加密加压后通过专用通道传送到云端存储。

## 结构化数据采集

### 信息采集方式

结构化信息采集采用前置或无前置两种模式。前置模式需要在医院部署独立数据采集设备，无前置模式需要把数据采集软件部署在医院服务器或工作站上。

#### 个人基础信息

通过满足但不限于IHE标准与REST标准来上传登记信息到云平台。无前置模式需要医院RIS具有前置信息登记采集能力。应包含的信息：病历号、患者姓名、身份证号、手机号码、年龄、性别、主诉等。

#### 检查信息

前置模式是医院RIS通过REST接口的方式来上传检查信息到云平台。无前置模式需要医院RIS具有前置检查信息采集能力。应包含的信息：医院编号、检查唯一标识、检查号、患者中文姓名、检查类型、检查部位、送检科室等。

### 报告采集

通过多种传输形式将审核完成的报告数据进行上传。应包含的报告数据信息：医院编号、检查编号、检查UID、患者编号、影像所见、影像所得等。

## 前置网关

前置网关是前置模式的重要组成部分，是一台物理设备，部署于医院内部，承担着从医院内部信息系统或医疗检查设备上采集必要的数据信息，经相关数据处理后上传到云端或反向从云端获取数据回传到院内信息系统的功能。

### 主要技术要求

——能够支持影像云平台端下发配置规则自动生效的功能；

——能够在影像云平台端监控采集设备及程序的运行状态；

——支持影像云平台端对各医院的采集程序一键升级；

——至少支持但不限于入库、归档、影像解析、加密、压缩、完整性校验等功能；

——支持加密传输结构化数据：采用HTTPS传输，敏感信息采用AES加密；

——支持物理文件上云、从云上回溯影像功能；

——支持影像跨院推送；

——根据DICOM标准协议从医院PACS系统或放射设备上获取影像信息。

# 数据传输规范

医学影像数据涉及到患者个人隐私，要求影像云所使用的线路需支持传输加密。医疗机构根据实际需求选用数字电路或SD-WAN的形式进行数据传输。数字电路应为医院提供安全、高效的专线连接，与互联网物理隔离；SD-WAN网关应采用互联网专线+IPSEC加密或其他密钥加密方式，保障影像数据在虚拟专网上传输的可靠性，完整性。

# 影像云平台技术规范

## 数据内容

### 主索引

主索引是区域内跨医疗机构、跨平台个人影像档案唯一主索引标识。主索引应包括：医疗机构编码、身份证号、检查号等。影像云平台将获取医疗机构编码、身份证号和检查号，以及影像访问地址发送给区域健康信息平台，区域健康信息平台以医疗机构编码，身份证号和检查号规则生成唯一主索引，同步到区域影像云平台。

应用方应基于授权，通过主索引方式，进行影像调用，实现互通，共享。

### 患者基本信息

患者基本信息进行结构化后存储到云端数据库。应包含的信息：患者主索引、患者姓名、性别、年龄、影像号、检查设备、检查部位、检查方法等。

### 检查信息

医院RIS系统上传患者检查信息到云平台。应包含的信息： 检查编号、患者id、检查UUID、检查日期、检查时间、检查类型、患者姓名、图像信息等。

### 报告数据

医院RIS系统将医疗机构审核完成并发布的报告数据上传到影像云平台。报告信息通过医院编码、检查id和患者检查信息关联，每一份患者检查信息只能关联一份报告，医疗机构修订报告后需要重新上传报告，影像云将会替换原先上传的报告。

### 影像数据

将所需的全序列化DICOM影像，包括但不限于CT、MR、DR、DX、CR等设备产生的影像，经过无损压缩，加密上传到影像云存储中。影像数据文件（DICOM）整体文件进行压缩，要求按每个子文件进行压缩。对于诊断级数据，应采用DICOM无损压缩。对于浏览级数据，可采用其他有效压缩算法。

## 数据存储

### 云计算要求

影像云平台应采用开放、兼容的弹性可扩展技术架构，实现网络、安全、计算、存储等基础设施的整合共享；基于先进的云计算架构和高性能的云计算技术，搭建细分资源类型和服务领域的系统模块，构建物理分散、逻辑集中的总分一体化云平台网络体系。

### 云存储要求

影像云平台需要大容量存储满足医学影像数据量大、且医患端长期调阅需求。为实现持续、全面、快速的综合数字影像信息获取，云存储应满足安全、高可靠的特性，具备多种存储类型供选择，包括块存储、对象存储等；云存储应具备较强的扩展能力，采用先进的磁盘容错技术，在硬盘故障后可实现快速重构，避免重构过程中其他硬盘损坏导致的数据丢失风险。

## 数据灾备

影像云数据中心应构建出相对隔离的网络环境（专有或者专属网），并划分出内网安全域和外网安全域。通过数据跨区域复制等技术，保障数据的高可靠性，防止数据丢失。建立异地备份数据中心，实现两地备份机制。

# 影像云平台安全规范

## 基本要求

按照《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等相关法律法规要求，落实影像数据安全责任。

按照《网络安全等级保护2.0版》三级标准进行建设，实现以应用为核心的安全防护系统，并在信息系统访问的全过程进行有效控制，全面提升信息系统的抗攻击能力，保障信息系统的高可用性和安全性。

——物理设施方面，具备数据中心管理和运营能力；

——传输层面，所有操作都可以通过HTTPS协议进行，确保数据传输过程进行加密以保证传输安全；

——数据访问控制策略和认证方面，云存储提供多种数据访问控制策略；

## 安全体系建设

——平台应部署边界防御类包含但不限于下一代防火墙，Web防火墙，入侵防御、防DDOS攻击；

——主机防御类包括但不限于漏洞扫描系统、网页防篡改；

——运维审计类包括但不限于数据库审计系统、堡垒主机系统、SSL VPN设备。

# 机房物理环境技术规范

根据上述技术要求，应提供省域内标准机房搭建专有云或私有云环境，有相应的安全及等保资质。机房应配有专有的机柜和配电，跟机房的其它非业务相关环境网络物理隔离。机房在选址、建筑结构、供电、制冷、消防、布线、物理访问控制、防盗防破坏等方面符合 GB 50174-2017 中第 8 章（电气要求）、第 10 章（网络与布线）、第 11 章（智能化系统）的要求，满足GB50174-2017有关A级机房的标准。

（1）规范性

数据中心应遵循国家有关法律、法规，执行国家A类数据中心有关规范标准，大于等于Tier3(或满足同等标准)，数据中心整体可用性必须达到99.982%以上（即全年不可用时间不超过1.6小时）；

（2）可靠性

数据中心具有抵御自然灾害如地震、火灾、水害、鼠虫害等的能力，能确保电力供应及空调运行的稳定性和连续性。

（3）可扩展性

数据中心的电力容量、空调容量、通讯能力等数据中心基础设施的各个方面都应预留足够的余量及可扩充的灵活性。

（4）安全性

数据中心应具有极高的安全性，包括人员出入控制、消防设施、供配电系统、空调系统、备用发电机系统、数据中心防电磁辐射干扰、防雷、防水、防静电等设施、环境监控系统等所有数据中心设施，在设计、配置和运行管理上均遵循严格的安全原则。