

# 医 保 影 像 云 基 础 规 范

---

## “医保影像云”基础规范

---

国家医疗保障局发布

## 前言

为统一规范医保影像云业务应用、基础设施建设、业务人员、医用设备及图像等基础性要求，特制定《医保影像云—业务应用规范》《医保影像云—基础设施技术规范》《医保影像云—业务人员、设备及图像基础要求》。

本规范起草单位：国家医疗保障局、中华医学会放射学分会、中国医学科学院北京协和医学院、四川大学华西医院、海军军医大学第二附属医院、首都医科大学附属北京友谊医院、上海交通大学医学院附属瑞金医院、北京大学。

本规范起草人：付超奇、曹文博、张雯、田梦楠、张子祺、郝文祥、孙嘉楠、陈盈艺、王灿琦、赵怡松、王振常、金征宇、刘士远、李真林、薛华丹、牛延涛、萧毅、严福华、李佳、周羽翀、王亚沙、周昌令、赵俊峰、刘学洋、胡文蕙。

# 目 录

《医保影像云—业务应用规范》 .....	1
一、适用范围 .....	1
二、定义 .....	1
三、总体建设要求 .....	3
四、总体建设架构 .....	4
五、适用场景 .....	5
六、影像中心技术要求 .....	7
七、前置机端技术要求 .....	11
八、个人端技术要求 .....	14
九、安全规范 .....	16
十、影像中心、前置机端影像检查图像浏览工具要求 .....	20
十一、个人端影像检查图像浏览工具要求 .....	23
《医保影像云—基础设施技术规范》 .....	28
一、适用范围 .....	28
二、定义 .....	28
三、物理环境要求 .....	28
四、硬件设备要求 .....	32
五、基础平台要求 .....	38
六、云服务要求 .....	38
七、网络要求 .....	39
八、安全防护要求 .....	43
九、容灾备份要求 .....	47
十、存储介质处置要求 .....	47
《医保影像云—业务人员、设备及图像基础要求》 .....	49
一、适用范围 .....	49
二、定义 .....	49
三、业务人员要求 .....	49
四、医学影像设备要求 .....	50
五、影像检查图像基础要求 .....	51

# 医保影像云—业务应用规范

## 一、适用范围

本规范明确了医保影像云业务应用场景、建设要求、建设架构、技术要求及安全规范。适用于各级医保部门、定点医疗机构、健康类人工智能服务机构、第三方技术服务机构，以及健康传感器服务机构开展医保影像云相关业务。

## 二、定义

**（一）医保影像云：**为解除群众疾病医疗后顾之忧，更好地维护医保参保人权益，依托全国医保信息平台，遵循医保技术与业务标准规范，运用云计算、大数据等技术，构建影像检查数据全国存储、机构调阅、参保人查阅的数字化服务平台，支撑全国定点医疗机构间影像检查数据的互通共享。

**（二）医保支付：**基本医疗保险基金依据国家法律法规及政策规定，对参保人员发生的符合医保目录范围的合规医疗费用，按标准予以给付的基金结算行为。

**（三）医保影像数据中心（以下简称“影像中心”）：**各省医保部门对辖区内定点医疗机构产生的影像检查数据进行集中存储、图像质控、数据管理、数据调度的系统。

**（四）前置机端：**部署于定点医疗机构前置机内，用于影像检查数据上传、缓存、调阅的系统。

**(五) 个人端：**为参保人提供影像检查数据查阅、分享等功能的系统。

**(六) 医疗机构信息系统：**定点医疗机构内部用于处理医疗业务、管理医疗数据、支撑诊疗活动的信息系统。

**(七) 影像检查数据：**医学影像检查中产生的影像检查基础信息、影像检查图像及影像检查报告的完整数据集合，即国家医保局《放射检查类医疗服务价格项目立项指南》中的检查资料<sup>1</sup>。

**(八) 影像检查基础信息：**“医保影像云索引”及数据集，包括证件类型、证件号码、检查日期时间、成像设备、检查部位、影像存储单位以及检查医院等级、检查项目、影像描述、诊断结果、结算 ID 等数据集。影像检查基础信息中的结算数据（结算 ID、费用明细流水号）须通过医保影像云索引与影像检查图像映射关联。

**(九) 影像检查图像<sup>2</sup>：**定点医疗机构提供医学影像检查服务，通过医学成像技术、后处理技术获得的人体内部结构和功能的可视化呈现。

**(十) 影像检查报告：**执业影像医师基于数字化影像编撰的标准化电子文书，包含检查概况、征象描述与诊断结论，属检查资料的组成部分，与原始影像、结算数据映射绑定并同步归档。

<sup>1</sup> 《放射检查类医疗服务价格项目立项指南》中“情况说明”第 17 条：“公立医疗机构开展相关放射检查须提供符合要求的‘数字影像处理和上传存储服务’并执行现行放射检查项目价格，实现患者可通过便捷方式阅读本人检查资料，同行可跨地区跨机构调阅检查资料，医保部门可核查已上传的检查资料；对于不能提供符合要求的‘数字影像处理和上传存储服务’的，执行的相关放射检查项目价格减收 5 元。”

<sup>2</sup> 包括：X 线摄影成像、计算机体层成像、磁共振成像等。

**(十一) 相同检查：**检查类型、检查部位、检查体位/扫描方式均一致的医学影像检查。

**(十二) 定点医疗机构：**自愿与统筹地区经办机构签订医保协议，为参保人员提供医疗服务的医疗机构。

**(十三) 健康类人工智能服务机构：**运用人工智能技术为影像检查提供数据处理、分析等服务的专业机构。

**(十四) 第三方技术服务机构：**为医保影像云建设、运营、维护提供技术支持、系统开发、服务保障等专业化服务的第三方机构。

**(十五) 健康传感器服务机构：**具备健康传感器产品研发、生产、销售资质，可向医保影像云提供合规健康数据接入服务的企业或机构。

### 三、总体建设要求

为保障医保影像云稳定、高效运行，满足各类业务场景以及未来业务的发展需求，系统建设与应用须符合统一性、可扩展性、可持续性、易用性、安全性的要求。

**(一) 统一性：**医保影像云须基于全国统一的医保信息平台，采用统一的技术规范、数据标准、交互方式，确保系统兼容、数据一致、业务协同。

**(二) 可扩展性：**医保影像云须支持模块化拆分与参数化配置，具备存储容量动态扩容和全生命周期数据兼容能力，确保可随用户规模、数据量、业务需求的变化灵活扩展。

**(三) 可持续性:** 医保影像云须在长期运行中保持功能、效率和适应性能力，确保技术、管理、经济等多维度持续优化。

**(四) 易用性:** 医保影像云须保障页面元素清晰呈现、操作流程简化设计、友好交互、明确反馈，确保用户良好使用体验。

**(五) 安全性:** 医保影像云须遵循 GB/T 22239-2019 《信息安全技术 网络安全等级保护基本要求》相关要求，评估医保影像云保护的信息资产和面临的威胁，构建安全防护体系。

#### 四、总体建设架构

医保影像云采用“1+32”层级化建设架构，以国家医保信息平台为基础，构建国家医保影像云索引共享模块，32个省级行政区域分别建设省级医保影像云。每个省级医保影像云均包含前置机端、影像中心、个人端三大核心组成部分。

其中前置机端主要用于影像检查数据上传、缓存，影像中心主要用于影像数据存储，个人端主要用于参保人查阅影像检查数据。



图 1 总体架构图

## 五、适用场景

适用场景包括：影像检查数据的上传、存储、缓存、调阅、参保人查阅等。

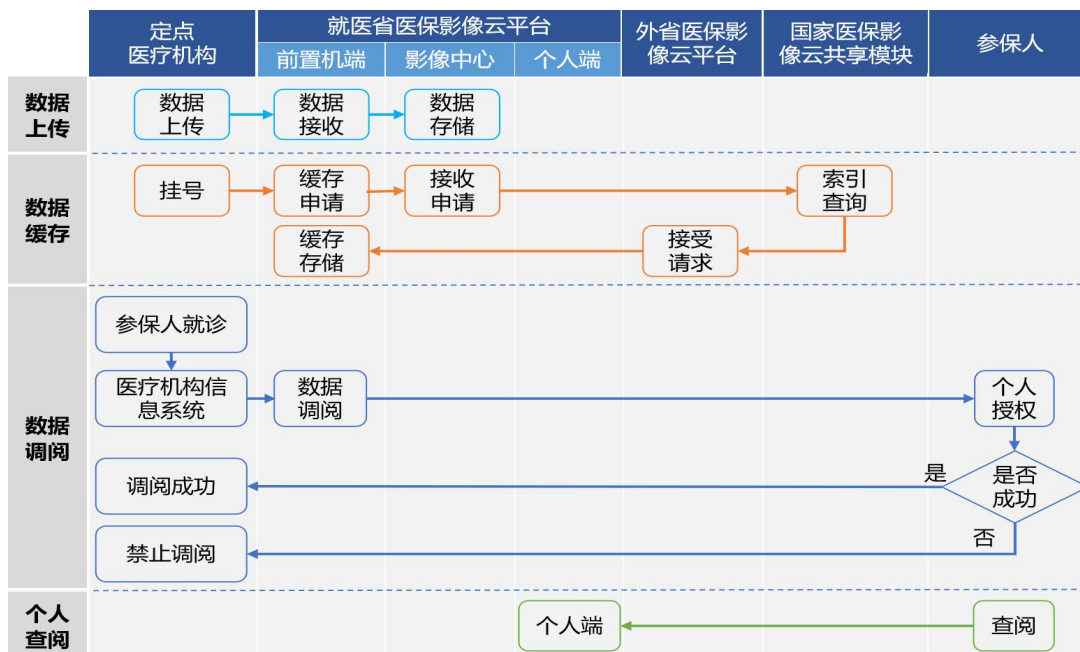


图 2 场景交互图

### (一) 影像检查数据上传与存储

定点医疗机构在提供医学影像检查服务时产生的影像检查数据，须自动上传至影像中心，影像中心接收并存储影像检查数据。

影像中心须预留接口，用于接收健康传感器服务机构、健康类人工智能服务机构上传的数据。

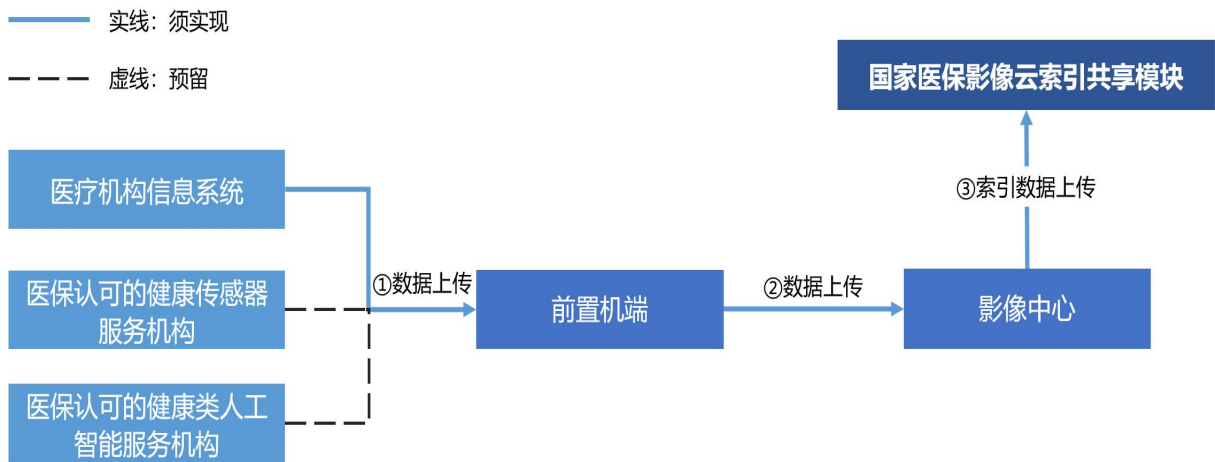


图 3 影像检查数据上传与存储

## (二) 影像检查数据缓存

参保人挂号后，前置机端缓存参保人就医省和外省的所有历史影像检查数据。



图 4 就医省影像检查数据缓存

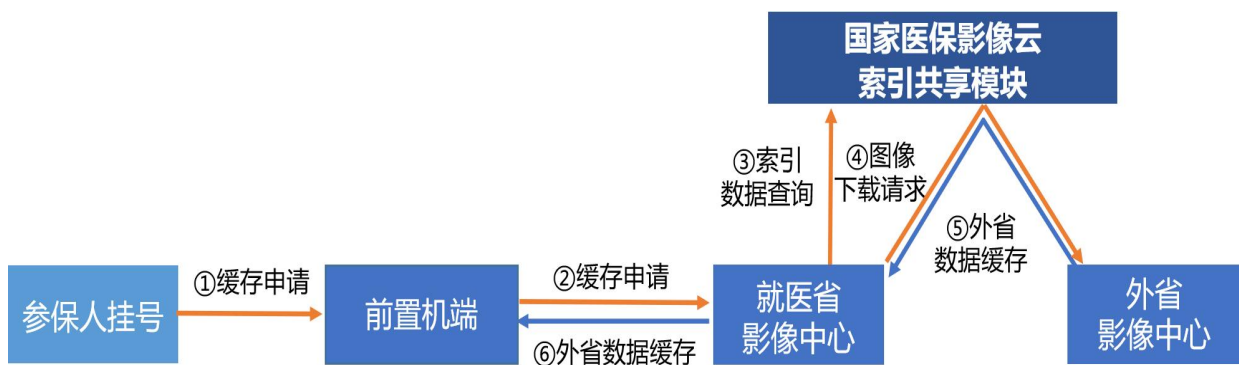


图 5 外省影像检查数据缓存

## (三) 影像检查数据调阅

医生在门诊、住院等临床诊疗过程中，经参保人授权后，可在医疗机构信息系统调阅参保人影像检查数据。

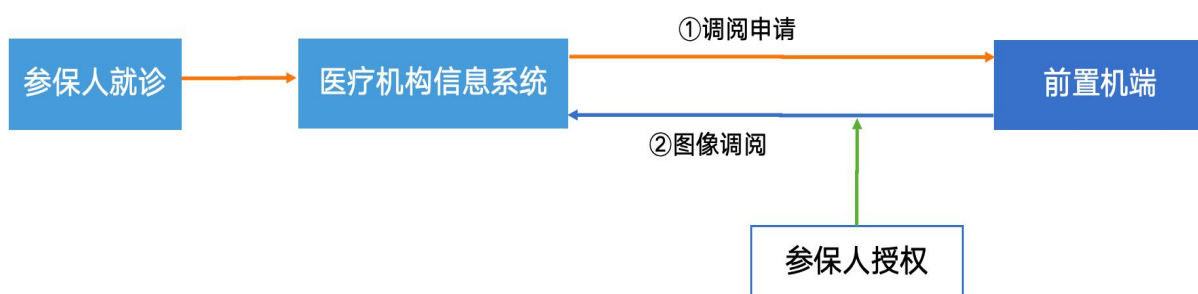


图 6 影像检查数据调阅

#### （四）参保人查阅影像检查数据

参保人通过身份验证后，可查阅、分享个人及亲情账户在就医省和外省的影像检查数据。

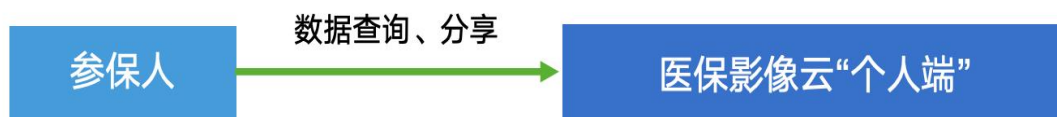


图 7 参保人查阅影像检查数据

## 六、影像中心技术要求

### （一）服务方式

影像中心须提供多种服务形式，包括：标准的RESTful API接口、软件开发工具包（SDK）、网页等。

### （二）功能要求

#### 1.数据传输

影像中心接收定点医疗机构前置机端上传的影像检查数据，

须满足如下要求：

（1）机构信息管理：医疗机构的基础信息管理，包括医疗机构名称、编码、等级等关键信息新增、删除、修改等功能；

（2）密钥管理：医疗机构数据传输加密密钥管理，包括密钥生成、修改、删除等功能；

（3）传输链路配置与监测：医疗机构数据传输网络链路的配置与监测，包括链路新增、编辑、删除、异常告警等功能。

（4）医保影像云索引上传：影像中心须依据《国家医疗保障局办公室关于开展医保影像云索引上传试点工作的通知》中相关要求，将影像检查数据上传至当地医保影像云索引共享模块。

（5）影像检查基础信息中的结算数据（结算 ID、费用明细流水号）须通过医保影像云索引与影像检查图像映射关联。

## **2.数据存储**

影像中心存储定点医疗机构前置机端上传的影像检查数据，须满足如下要求：

（1）存储策略配置：影像检查数据存储参数配置，包括存储路径配置、告警阈值配置等功能；

（2）存储容量监控：影像检查数据存储的监控，包括存储容量使用率监控、存储容量展示、异常告警等功能；

（3）存储用量统计：数据存储容量使用情况多维度的统计、展示，包括检查模式、检查时间等维度。

## **3.数据应用**

影像中心管理影像检查数据的应用，须满足如下要求：

（1）编码标准化管理：医疗机构检查项目编码与医保影像检查项目编码的映射管理，包括编码映射、编辑、删除等功能；

（2）调阅管理：医疗机构调阅影像检查数据的全流程管理，包括调阅频次统计、调阅率评估等；

（3）业务记录管理：医疗机构在数据上传、调阅等业务过程中产生的记录，包括缓存申请记录、数据上传监测记录、调阅记录、下载记录、挂号记录、个人端分享记录等信息；

（4）操作日志管理：用户在使用系统过程中产生的记录，包括操作用户、操作类型、操作时间等信息。

#### **4.图像质控**

影像中心须满足如下要求：

（1）为患者付费、医保支付、基金监管、临床诊疗、大数据分析应用等场景提供符合《医保影像云—业务人员、设备及图像基础要求》中相关要求的影像检查图像；

（2）依据《医保影像云—业务人员、设备及图像基础要求》，对前置机端上传的影像检查图像进行质量控制；

（3）将影像检查图像质控结果告知上传及调阅的定点医疗机构；

（4）鼓励采用人工智能技术辅助开展影像检查图像质量控制工作。

#### **5.数据缓存申请处理**

影像中心须满足如下要求：

(1) 为前置机端提供数据缓存申请处理服务，接收并记录前置机端发起的影像检查数据缓存申请；

(2) 接收前置机端影像检查数据缓存申请时，优先检索本省存储的影像检查数据。若数据存在，前置机端直接缓存；若数据不存在，则向国家医保影像云索引共享模块发起影像索引信息查询申请，依据返回的影像索引信息，向外省影像中心请求数据缓存并由前置机端直接缓存。

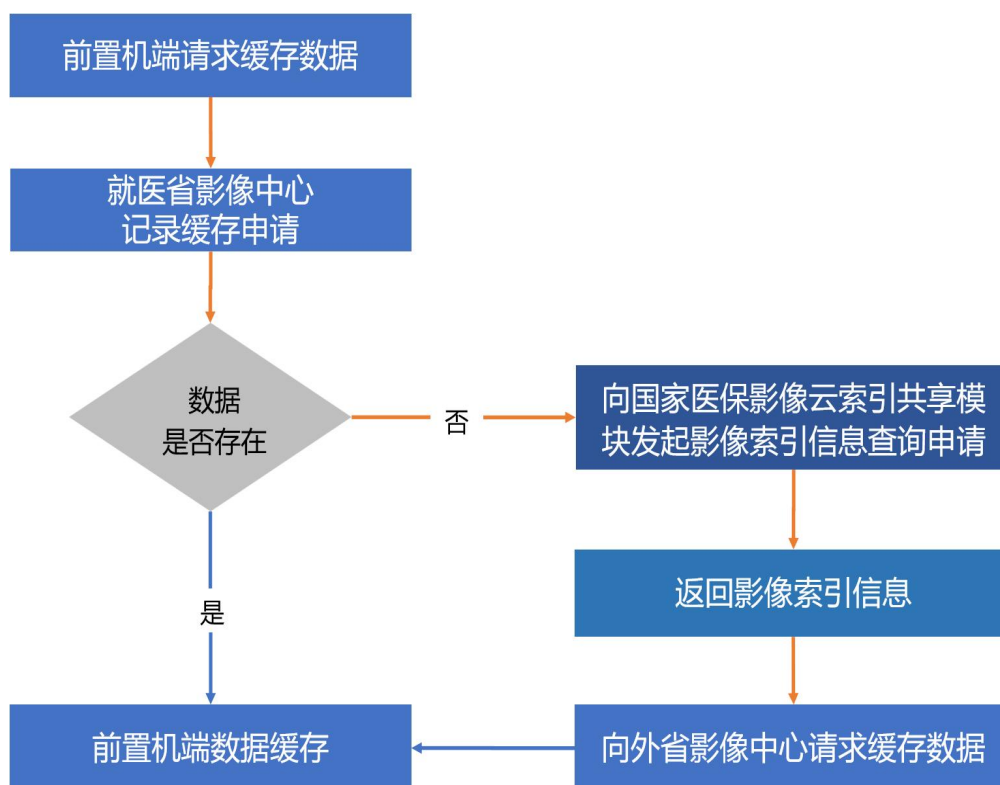


图 8 影像检查数据缓存申请处理

## 6.数据调阅

影像中心须满足如下要求：

(1) 具备影像检查数据浏览工具，且界面中须包含“中国医疗保障”标识和“医保影像云索引”，其功能、样式、布局参考附录《影像检查图像浏览工具样式布局及功能要求》。

(2) 调阅过程中须保障急诊患者优先调阅。

## **7.数据监测**

影像中心须自动监测上传的影像检查数据，确保数据完整性、有效性、时效性，将监测结果动态反馈至前置机端，并根据反馈结果触发数据重传、补传机制。

### **(三)性能要求**

#### **1.存储期限**

自医学影像检查完成时起，门（急）诊影像检查数据须存储15年，住院影像检查数据须存储30年。影像检查数据可采用分层存储策略：

(1) 热存储：检查完成之日起1年内的数据；

(2) 温存储：检查完成之日起1年至3年内的数据；

(3) 冷存储：检查完成之日起3年以上的数据。

已达到存储期限的影像检查数据，可按需延长存储期限。

#### **2.并发性能**

影像中心应具备满足业务峰值需求的并发支撑能力，保障影像检查数据稳定上传与查询等业务。

## **七、前置机端技术要求**

### **(一)服务方式**

前置机端须提供影像检查数据上传、调阅、缓存等多种服务，服务方式包括：标准的RESTful API接口、软件开发工具包(SDK)、独立插件、页面嵌入等。

## **(二) 功能要求**

### **1.数据上传**

定点医疗机构须依据《影像检查数据上传服务接口文档》要求，实现影像检查数据应传尽传。前置机端在数据上传时须满足如下要求：

(1) 影像检查基础信息中的**结算数据**（**结算 ID、费用明细流水号**）须通过**医保影像云索引与影像检查图像映射关联**。

(2) 影像检查图像符合DICOM 3.0及以上版本标准；

(3) 依据DICOM 3.0及以上版本标准，对上传的影像检查图像进行无损压缩处理；

(4) 须将经后处理生成的3D序列影像检查图像与原扫描图像一并上传<sup>3</sup>；

(5) 在影像检查报告出具后24小时内完成影像检查数据上传，急诊患者优先上传；

(6) 具备影像检查数据上传自动监测机制，对漏传、错传的数据，自动补传、自动重传。

### **2.数据缓存**

医疗机构应在参保人挂号环节，获得参保人历史检查数据缓

<sup>3</sup> 例：肋骨的三维重建图像须与肋骨 CT 平扫图像共同上传。

存授权。须在挂号界面明确告知参保人历史检查数据缓存事宜，由参保人确认完成授权。前置机端数据缓存须满足如下要求：

（1）参保人挂号完成后，医疗机构信息系统自动触发前置机端向就医省影像中心发起缓存申请。缓存信息需包含参保人个人身份信息（如姓名、证件类型、证件号码等）、就诊信息（如挂号科室、就诊时间等）。所有挂号记录、缓存下载记录须上传至医保影像云索引共享模块。

（2）参保人预约挂号，前置机端须保障在参保人就诊前1日晚，完成历史影像检查数据缓存。

（3）参保人当日挂号，前置机端须在挂号后10分钟内，完成历史影像检查数据缓存。

（4）前置机端须自动监测缓存失败的影像检查数据，并触发重新缓存机制，重新缓存次数不得少于3次。

### **3.数据调阅**

前置机端须满足如下要求：

（1）医生接诊时，前置机端须自动提醒就诊参保人在定点医疗机构的历史影像检查数据。

（2）医生为参保人开具检查医嘱时，前置机端须依据检查医嘱，自动提醒当前参保人历史影像检查数据中的所有相同检查。

（3）医疗机构信息系统调阅参保人影像检查数据时，展示信息须包括：影像检查报告、影像检查图像、影像质控结果。

（4）医疗机构信息系统调阅参保人影像检查数据时，须获

取个人授权，授权方式可采用医保码授权（含医保码亲情账户授权）、医保服务平台APP授权、医师辅助授权<sup>4</sup>、电子签名授权、医保IOT终端刷脸授权、短信验证码、APP令牌、生物特征（如刷脸）、书面授权等任一方式。所有调阅记录须上传至医保影像云索引共享模块。

（5）须配备影像检查数据浏览工具，须包含“中国医疗保障”标识和“医保影像云索引”，其功能、样式、布局参考附录《影像检查图像浏览工具样式布局及功能要求》。

### （三）性能要求

#### 1.调阅速度

医疗机构信息系统调阅影像检查图像时，首幅图像须在3秒内完整显示；计算机断层扫描（CT）、磁共振成像（MRI）每10幅图像加载时间不超过1秒<sup>5</sup>。

#### 2.缓存期限

前置机端影像检查数据缓存期限，自最近一次就诊时间起算<sup>6</sup>，数据须存储不少于3天，可结合实际情况，灵活延长缓存时限。到期需删除缓存文件，并留存删除日志。

## 八、个人端技术要求

### （一）服务方式

<sup>4</sup> 在参保人因年龄、身体状况、认知障碍或其他特殊原因难以独立完成电子或书面授权操作时，经参保人本人知情同意后，由执业医师通过扫码、代操作设备等合规方式，协助参保人完成授权。

<sup>5</sup> 例：单幅图像大小 $\leq 300\text{kb}$ 情况下，1秒钟下载10幅图像。

<sup>6</sup> 例：某人就诊于2025年10月15日，缓存至少存储到2025年10月18日24:00。

个人端可通过国家医保服务平台、二维码、网页链接、公众号、小程序、APP等多类入口查阅个人影像检查数据。该服务支持跨平台访问，可自适应手机、平板等终端设备，且兼容HarmonyOS、iOS、Android等主流操作系统。

## （二）功能要求

个人端须具备影像检查数据的查看、分享等功能。

**1.查阅功能：**个人端须具备查阅参保人及亲情账户在就医省和外省影像检查报告、影像检查图像等功能。参保人查阅外省影像检查图像时，须由参保人发起申请，经就医省影像中心向外省发起调取并完成缓存后方可查阅。

**2.分享功能：**个人端须提供二维码、链接等多种分享途径，分享时可设置分享密码、有效期限、查看次数等权限参数。同时支持参保人查看分享记录（包括分享期限、查看次数、分享时间等信息）、撤销分享操作（撤销后对应的影像检查数据将无法访问<sup>7</sup>）。

**3.影像检查图像浏览：**个人端须具备影像检查图像浏览工具，须包含“中国医疗保障”标识和“医保影像云索引”，其功能、样式、布局参考附录《影像检查图像浏览工具样式布局及功能要求》。

## （三）性能要求

**1.查阅速度：**个人端在查阅JPG/PNG格式影像检查图像时，

<sup>7</sup> 仅针对该分享途径（二维码、链接等）的访问权限限制。

首幅图像完整显示响应时间须在 3 秒内；调阅 DICOM 格式影像检查图像时，在用户确认调阅操作后，首幅图像完整显示响应时间须在 5 秒内。

## **九、安全规范**

医保影像云建设须通过国家信息安全等级保护第三级测评，保障系统运行、存储、传输及个人信息安全。

### **（一）身份鉴别**

医保影像云须满足如下要求：

1.对所有访问用户实施严格的身份核验机制，确保用户身份真实合规，防范非法访问风险；

2.严禁采用默认口令、弱口令等不安全身份验证方式。对于需采用身份鉴别的用户角色或场景，须启用多因素认证（MFA），可通过医保码、短信验证码、APP令牌、个人身份信息或生物特征（如刷脸）等方式完成二次身份校验。

### **（二）访问控制**

医保影像云须满足如下要求：

1.依据“业务必需”和“最小权限”原则，为不同角色用户（如系统管理员、医疗机构管理员、医生、个人等）分配不同的数据访问和操作权限；

2.对影像检查数据、影像检查报告、个人身份信息等重要资源设置敏感标记，并基于安全策略严格控制相关操作。

### **（三）安全审计**

医保影像云须满足如下要求：

1.具备完备的安全审计功能，对用户登录、数据上传、数据调阅等关键操作及异常事件进行全程日志记录；

2.审计记录须包括：操作时间、操作用户、事件类型、操作结果等核心要素，且需按规范定期备份，留存期限不得少于6个月；

3.安全审计日志须配置严格的访问控制策略，同时采用日志签名、转发至不可变存储日志中心等防篡改技术，保障日志的真实性、完整性，防止未经授权的访问、删除或修改行为。

#### **（四）数据完整性**

医保影像云须满足如下要求：

1.在数据传输与存储过程中，应采用哈希校验等技术确保完整性。所有通过公共网络或不安全网络传输的数据（包括API调用、网页访问、数据上传下载），须使用行业公认的安全协议进行加密；

2.在影像检查数据上传时须采用经济可行、安全可靠的加密方式进行加密防护，缓存时进行解密校验，严防数据非法篡改，保障数据全程可信；

3.具备存储数据完整性的自检和修复机制。

#### **（五）个人信息保护**

医保影像云须满足如下要求：

1.处理个人信息前，须依法取得个人同意，并通过隐私政策等合规形式，明确告知处理目的、方式、信息种类、保存期限、

权利行使途径等；

2.遵循“目的明确、最小必要、公开告知、个人授权”原则，严格控制个人信息收集、存储、使用、共享；

3.对个人信息进行去标识化处理，加强访问控制管理；

4.严格区分数据使用场景：用于临床诊疗、医保支付等业务的数据，应按“最小必要”原则进行去标识化处理；用于人工智能训练、大数据分析、科学研究等二次利用的场景，须对个人信息进行不可逆匿名化处理，或依法取得个人同意。

#### **（六）数据存储安全**

医保影像云须满足如下要求：

1.影像检查数据的静态存储须采取加密措施；

2.前置机端的缓存数据，应在达到本规范规定的最短缓存期限后，按预设策略自动清理，避免敏感信息在临时环境长期滞留；

3.影像检查数据未经省级及以上医保主管部门批准，任何单位和个人不得挪作他用；

4.建立完善的数据备份与恢复机制，定期备份重要数据，确保数据损坏或丢失后可及时恢复；

5.建立安全的密钥管理机制，用于数据加解密的密钥须妥善存储、保护（例如使用硬件安全模块（HSM）或受信任的密钥管理服务（KMS）），且密钥的生命周期（生成、存储、分发、轮换、销毁）应严格遵照安全规范执行。

#### **（七）网络安全防护**

医保影像云须满足如下要求：

1.影像中心核心应用系统、数据存储系统与外部网络访问区域应进行严格的网络隔离，例如使用虚拟私有云（VPC）和安全组策略，仅开放业务必需的端口和服务；

2.部署网络防火墙和Web应用防火墙（WAF），对来自互联网的访问流量进行过滤和监测，防御常见的网络攻击（如SQL注入、XSS、DDOS攻击等）；

3.部署入侵检测系统（IDS）或入侵防御系统（IPS），对网络流量和主机行为进行实时监控，及时发现和阻断恶意渗透行为。

#### **（八）API 安全**

1.所有API接口必须进行严格的认证和授权。对API的调用应使用令牌（Token）、OAuth 2.0或同等级别的安全机制，确保每次调用的合法性。API授权应遵循“最小权限”原则；

2.须对API的调用频率进行限制（Rate Limiting）和并发控制，防止因滥用或恶意调用（如撞库、暴力破解）导致的服务拒绝（DoS）。

## 附录

### 影像检查图像浏览工具样式布局及功能要求

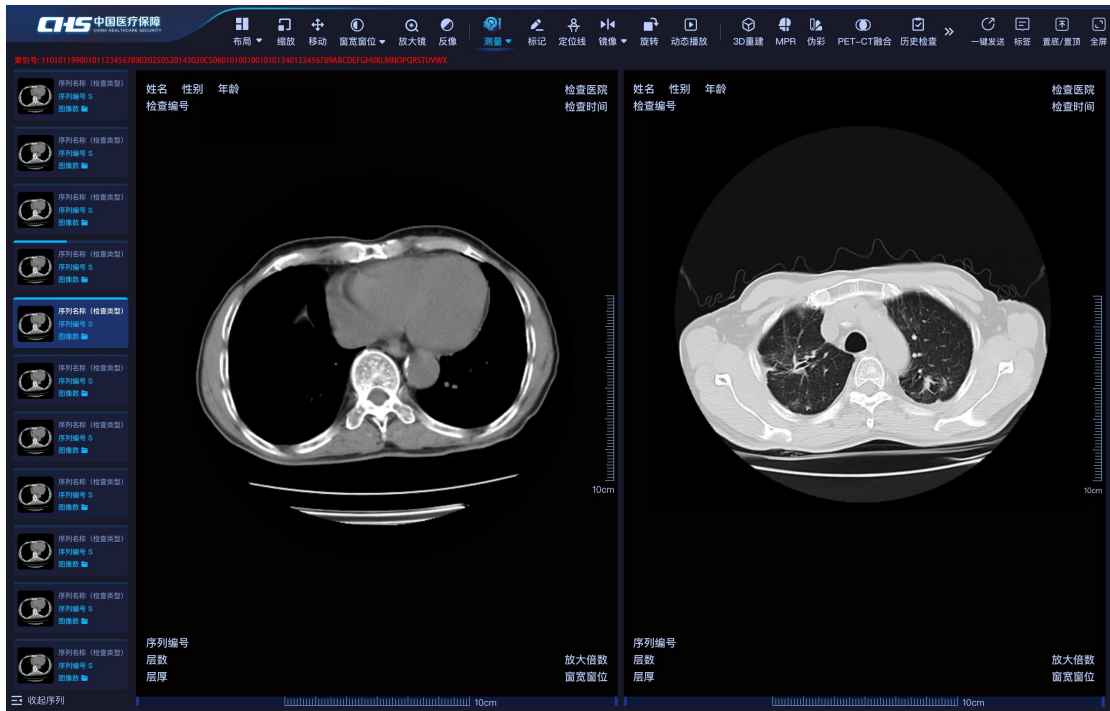


图 10 页面设计图（参考）

#### 十、影像中心、前置机端影像检查图像浏览工具要求

影像中心、前置机端的影像检查图像浏览工具须包含“中国医疗保障”标识（尺寸为328px × 233px）以及“医保影像云索引”（字号为20px，字体为黑体，颜色为红色）；支持专业设备浏览、多点触控交互，采用分区域样式布局，具体如下：

##### （一）功能操作

页面设计上方为功能操作区域，需集成临床阅片所需的基本

功能，包括：

- 1.鼠标快捷功能：左键按住可放大缩小、中键按住可移动、右键按住可调整窗宽窗位；
- 2.布局：支持序列布局调整、图像布局自定义功能；
- 3.缩放：支持图像放大缩小查看；
- 4.移动：支持移动图像位置以查看不同区域；
- 5.窗宽窗位：支持调节影像的灰度范围和中心灰度值，并支持快速调用预设标准窗宽窗位参数；
- 6.放大镜：支持影像局部区域进行实时放大；
- 7.反像：支持反转影像的明暗色调；
- 8.测量：支持直线测量、矩形测量、椭圆测量、角度测量等常规测量，以及COBB角测量、自由测量、CT值测量、心胸比测量等功能；
- 9.标记：支持在影像关键位置做标注说明；
- 10.定位线：在影像上叠加标识位置的定位线；
- 11.镜像：支持水平镜像、垂直镜像；
- 12.旋转：支持影像按顺时针/逆时针方向转动；
- 13.动态播放：按顺序连续播放序列影像，呈现动态效果；
- 14.MPR：支持冠状位、矢状位、轴状位重建影像；
- 15.MIP：支持最大密度投影图像处理功能；
- 16.MinIP：支持最小密度投影图像处理功能；
- 17.伪彩：支持用伪彩增强影像的细节对比；

18.PET-CT融合：支持整合PET功能影像与CT解剖影像；

19.历史检查：支持同一影像浏览界面对比浏览同一个人不同医疗机构、不同时期的影像检查图像；

20.一键发送：支持将DICOM图像一键发送至专业影像浏览设备进行操作浏览；

21.标签：支持查看DICOM图像参数信息；

22.功能栏置底/置顶：支持功能栏调整至图像浏览界面的下方/上方显示。

## **(二) 导航条信息**

页面设计图左侧部分为导航条信息展示区域，呈现影像检查图像关键信息，包括：

1.检查类型：清晰标注CT、DR、MRI等影像检查类型；

2.序列缩略图：支持可视化预览，以缩略图形式呈现各影像序列；

3.序列名称：以文字性描述标注序列信息；

4.序列编号：显示当前影像检查图像的序列编号；

5.序列图像数：显示当前序列包含的图像总数量。

## **(三) 图像展示**

页面设计图中间部分为图像展示区域，须支持DICOM图像清晰浏览，且固定显示角信息，包括：

1.图像展示：显示影像检查DICOM图像；

2.四角信息：用于阅片时核对影像检查图像关键信息（如设

计图所示)。

## 十一、个人端影像检查图像浏览工具要求

个人端影像检查图像浏览工具须包含“中国医疗保障”标识(尺寸为328px×233px)以及“医保影像云索引”(字号为20px,字体为黑体,颜色为红色);支持JPG/PNG格式图像浏览和DICOM格式图像浏览。默认加载并展示JPG/PNG格式图像;若用户需调阅DICOM格式图像时,须有提示确认<sup>8</sup>,具体如下:

### (一) JPG/PNG 格式图像浏览页面要求

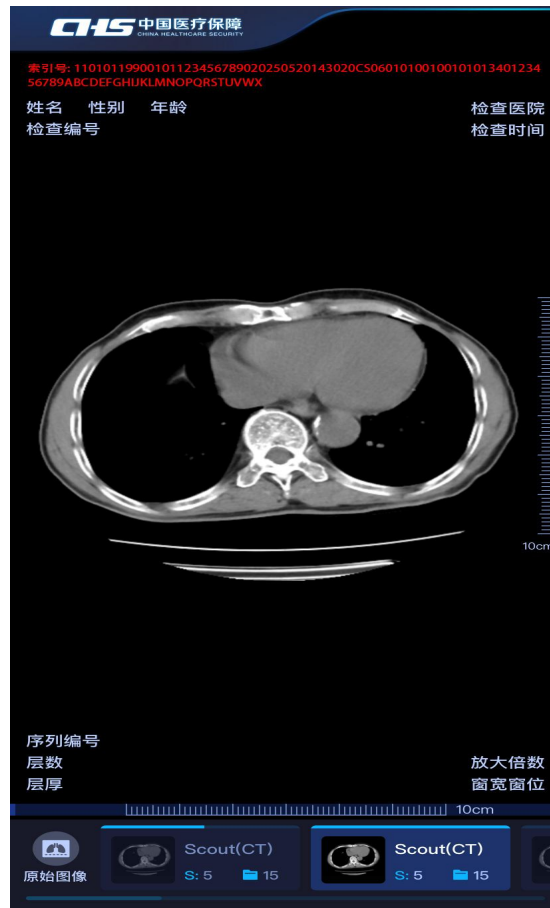


图 11 JPG/PNG 格式设计页面(参考)

<sup>8</sup>例:“DICOM 格式影像需消耗较多流量,是否继续调阅?”。

## 1.图像展示

JPG/PNG 格式页面中间部分为图像展示区域，支持 DICOM 图像清晰浏览，且固定显示四角信息，包括：

- (1) 图像展示：显示影像检查 DICOM 图像；
- (2) 四角信息：显示影像检查图像关键信息(如设计图所示)。

## 2.导航条信息展示

JPG/PNG 格式页面下方为导航条信息展示区域，呈现影像检查图像关键信息，包括：

- (1) 检查类型：清晰标注 CT、DR、MRI 等影像检查类型；
- (2) 序列缩略图：支持可视化预览，以缩略图形式呈现各影像序列；
- (3) 序列名称：以文字性描述标注序列信息；
- (4) 序列编号：显示当前影像检查图像的序列编号；
- (5) 序列图像数：显示当前序列包含的图像总数量。

### (二) DICOM 格式图像浏览页面要求

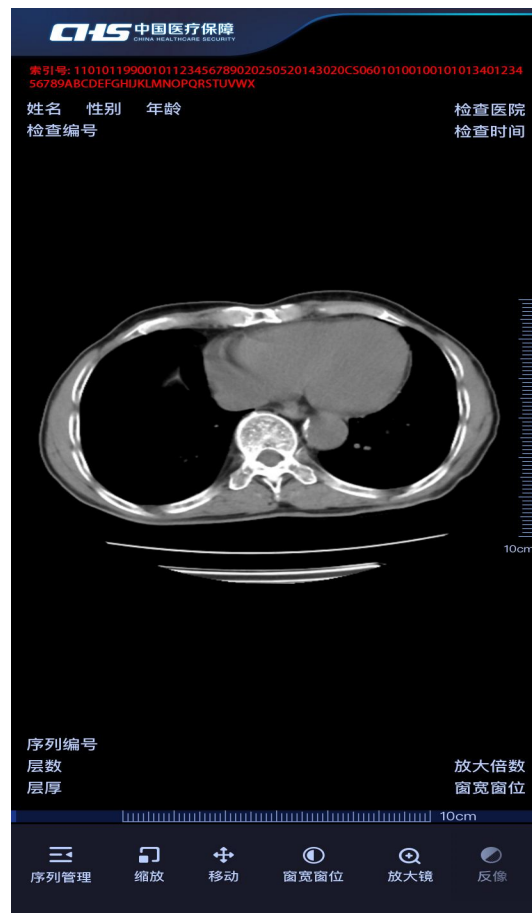


图 12 序列管理设计图（参考）

图 13 DICOM 格式设计图（参考）

## 1. 图像展示

DICOM格式页面中间部分为图像展示区域，支持DICOM图像清晰浏览，且固定显示四角信息，包括：

- （1）图像展示：显示影像检查DICOM图像；
- （2）四角信息：显示影像检查图像关键信息(如设计图所示)。

## 2. 功能操作

DICOM格式页面下方为图像展示区域和功能操作区域，集成临床阅片所需的基本功能，包括：

(1) 序列管理：支持导航条信息展开/收起功能，展示影像检查图像关键信息，包括：检查类型、序列缩略图、序列名称、序列编号、序列图像数量等；

(2) 导航条信息展开/收起：默认收起，展开后可展示检查序列，缩略图、序列名称、序列编号及序列图像数量等；

(3) 基础浏览操作：支持双指缩放控制，单指移动及动态播放等触控交互功能；

(4) 缩放：支持图像放大缩小查看；

(5) 移动：支持移动图像位置以查看不同区域；

(6) 窗宽窗位：支持调节影像的灰度范围和中心灰度值，并支持快速调用预设标准窗宽窗位参数；

(7) 放大镜：支持影像局部区域进行实时放大；

(8) 反像：支持反转影像的明暗色调；

(9) 测量：支持直线测量、矩形测量、椭圆测量、角度测量等常规测量，以及COBB角测量、自由测量、CT值测量、心胸比测量等功能；

(10) 标记：支持在影像关键位置做标注说明；

(11) 定位线：在影像上叠加标识位置的定位线；

(12) 镜像：支持水平镜像、垂直镜像；

(13) 旋转：支持影像可按顺时针/逆时针方向转动；

(14) 动态播放：按顺序连续播放序列影像，呈现动态效果；

- (15) 伪彩显示: 支持用伪彩增强影像的细节对比;
- (16) MPR: 支持冠状位、矢状位、轴状位重建影像;
- (17) MIP: 支持最大密度投影图像处理功能;
- (18) MinIP: 支持最小密度投影图像处理功能。

# 医保影像云—基础设施技术规范

## 一、适用范围

本规范明确了医保影像云在物理环境、硬件设备、基础平台、网络架构、安全防护、容灾备份、存储介质处置等方面的技术要求。适用于各级医保部门、定点医疗机构、第三方技术服务机构等。

## 二、定义

**（一）医疗保障核心业务区网络：**由国家医疗保障局统一规划，承载医疗保障核心业务数据交换的专用、安全网络。

**（二）医保影像云专网：**承载各级医保影像云影像检查数据高效、安全传输与调阅的专用广域网络。

## 三、物理环境要求

### （一）机房基础

#### 1.建设等级

数据中心机房规划与建设应遵循GB 50174-2017《数据中心设计规范》相关规定。等级划分要求如下：

（1）A级标准：适用于国家医保影像云；

（2）B级及以上标准：适用于各省级医保影像云、三级定点医疗机构；

（3）C级及以上标准：适用于三级以下定点医疗机构。

#### 2.功能区域

机房应明确划分用于安装和运行服务器、存储、网络等核心信息技术设备的主机房，用于设备的安装、调试、维护、运行监控和管理的辅助区，用于为主机房和辅助区提供动力支持和安全保障的支持区。

### **3.机房选址**

(1) 应远离强振源、强噪声源、强电磁场干扰源、易燃易爆品仓库及高污染源等环境敏感区域；

(2) 应避开机场、军事基地、政府要害部门、危险品仓库、化工厂、学校等特殊场所及地势低洼区域，周边需具备完善的交通、供电、网络、给排水等基础配套条件；

(3) 若机房设置在多层或高层建筑内，宜优先选择较低楼层，其楼面承重标准不应低于 $800\text{kg}/\text{m}^2$ ，且需避开卫生间、茶水间等存在水管泄漏风险区域的正下方。

### **4.温湿度与环境**

(1) 主机房在设备开机运行时，温度应控制在 $23^{\circ}\text{C} \pm 2^{\circ}\text{C}$ ，相对湿度应控制在30%~70%；

(2) 应配置专用精密空调系统，确保温湿度稳定，并维持机房内正压。机柜布局宜采用冷热通道方式进行隔离；

(3) 宜配置具备高效过滤功能的洁净新风机组，以保障机房空气洁净度。

### **5.消防设施**

(1) 应配置符合GB 50116-2013《火灾自动报警系统设计规范》要求的极早期火灾自动报警系统；

(2) 主机房应配置对电子设备无害的气体灭火系统（如IG541、七氟丙烷），并与火灾探测器、空调、门禁等系统进行联动控制；

(3) 设置气体灭火的机房，应在指定位置配置专用空气呼吸器或氧气呼吸器，并在入口处设置灭火显示灯和声光报警器。

## 6.网络布线

(1) 传输介质：核心主干链路光缆应采用OM3及以上规格的多模光缆或单模光缆；水平链路电缆应采用六类及以上屏蔽/非屏蔽对绞电缆；

(2) 防火等级：布线电缆应采用CMP（增压级）或CMR（干线级）防火等级，光缆应采用OFNP或OFCP防火等级；

(3) 走线方式：双绞线和光缆宜采用机柜上方（上走线）桥架或线槽进行布放，并与强电线缆保持安全距离；

(4) 配线管理：每列机柜宜设置列头配线柜，用于汇聚本列机柜线缆。

## 7.不间断电源

(1) 应配置N+1或2N冗余架构的在线式不间断电源，满载后备时间不少于30分钟，各省可根据实际情况延长满载后备时间；

(2) 核心业务设备应由不间断电源系统供电，并采用双路

供电模式；

(3) 各级医保影像云应配置柴油发电机作为备用电源；

(4) 三级定点医疗机构可根据实际情况配置柴油发电机。

## **8.防静电及防雷接地**

(1) 地面应铺设防静电地板，其系统电阻应在 $1.0 \times 10^6 \Omega \sim 1.0 \times 10^9 \Omega$ 范围内；

(2) 应遵循GB 50057-2010《建筑物防雷设计规范》和GB 50343-2012《建筑物电子信息系统防雷技术规范》要求，构建有效的多级防雷和等电位联结接地系统。

## **9.动力与环境监控系统**

应遵循GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》、GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，部署机房动力与环境集中监控系统，对UPS、配电柜、精密空调、温湿度、漏水、门禁状态、烟感等进行7×24小时实时监测、数据记录和分级告警。

### **(二) 安防管理**

#### **1.视频监控**

(1) 监控范围应全面覆盖机房出入口、机房内部通道、核心设备机柜区域，确保无监控死角；

(2) 视频录像资料保存时间不少于180天，视频清晰度不低于720P，视频帧率不低于25帧/秒，具备红外夜视功能。

## **2.出入管理**

(1) 应对机房出入口、监控室、安防设备间、变配电室、UPS电池室、发电机房、动力站房等所有关键区域实施严格物理访问控制；

(2) 门禁系统宜采用非接触式IC卡、生物特征识别（如指纹、人脸）或组合认证方式。

## **3.入侵监控**

(1) 应在机房内部、变配电室、UPS电池室、发电机房、动力站房等关键区域部署红外、微波等入侵探测装置；

(2) 报警系统应与监控中心联动，并能通过网络、电话或短信等方式及时通知安全管理人员。

## **四、硬件设备要求**

### **(一) 服务器设备**

在满足功能、性能、安全、可靠性及兼容性要求的前提下，服务器宜优先选用主流国产芯片及国产品牌。

#### **1.各省医保影像云服务器应满足如下要求：**

平台服务器配置需符合市场主流参数标准，具备高可用、高并发、低延迟、易扩展等特性，能够满足全国范围内医保影像数据7×24小时持续调用的业务需求，同时支持虚拟化平台、数据库、中间件等多种应用服务的统一部署。平台存储总可用容量需满足医保影像数据未来3—5年的增长需求，并保证日常运行水

位(已用容量/总可用容量)不超过70%。根据本省实际测算情况,支持存储配置动态调整。

## 2.医疗机构前置机应满足如下要求:

### (1) CPU 参数

①处理器:应采用多核处理器,支持64位计算,主频不低于1.8GHz。

②核心数:单颗物理CPU核心数量不少于4核。

### (2) 内存参数

①类型:应采用DDR4 3200MHz或更高规格纠错码内存。

②容量:单台前置机内存总容量不低于16GB。

③扩展性:内存插槽应具备扩展能力,以满足未来业务增长扩展需求。

### (3) 硬盘与 RAID 控制器

①系统盘:应配置2块容量不低于240GB的企业级固态硬盘,并配置为RAID 1;

②数据盘:可根据业务对I/O性能需求,灵活配置数据硬盘;

③RAID 控制器:应配置独立硬件RAID卡,支持RAID 0/1/5/6/10,板载缓存不低于2GB,并配备掉电保护模块。

(4) 网络接口:提供不少于2个千兆及以上网口。

### (5) 电源与管理

①电源:应配置1+1冗余热插拔电源;

②管理：应具备独立远程管理端口，支持带外远程控制能力和远程虚拟介质功能。

### **3.GPU 加速服务器<sup>9</sup>**

(1) GPU卡：应配置支持FP32/FP16/INT8等多种精度计算的高性能计算卡，单卡显存不低于12GB；

(2) CPU：应配置与GPU性能相匹配的高主频、高核心数CPU，避免成为性能瓶颈；

(3) 总线：应支持PCIe 4.0或更高版本的总线，为CPU与GPU之间提供足够的数据传输带宽；

(4) 散热：应具备针对GPU优化的散热设计，确保在高负载下长期稳定运行。

## **(二) 存储设备**

### **1.通用要求**

(1) 架构：可根据业务场景、性能和扩展性要求选用集中式SAN/NAS存储或分布式存储；

(2) 控制器：应采用全冗余架构，控制器应为Active-Active（双活）模式，确保无单点故障。

### **2.控制器参数**

(1) 缓存：单控制器缓存容量不低于64GB；

(2) 协议：应至少支持FC、iSCSI、NFS、CIFS、S3等协议

<sup>9</sup> 如配置 GPU 服务器，应符合此要求。

中的两种，以适应不同应用场景。

### **3.端口配置**

(1) 前端端口：每个控制器接口数不少于4个，接口速率不低于16Gb FC端口或10Gb iSCSI端口；

(2) 后端端口：应采用不低于12Gb/s的SAS 3.0通道连接磁盘柜。

### **4.硬盘配置**

(1) 类型：支持SSD、10K/15K RPM SAS、7.2K RPM NL-SAS等多种类型硬盘，并支持在同一存储池中混合配置；

(2) 数据冗余：应具备数据冗余保护能力，支持多种冗余配置（镜像、条带、奇偶校验等），并可根据数据重要性动态调整冗余级别。

### **5.系统功能**

(1) 数据保护：应具备快照、克隆、远程复制、双活、自动精简配置、服务质量控制等高级数据服务功能；

(2) 静态数据加密：所有存储系统应启用静态数据加密功能，宜支持密钥管理互操作性协议。

### **6.存储分层策略**

自影像检查完成时起，门（急）诊影像检查数据须存储15年，住院影像检查数据须存储30年，影像检查数据可采用分层存储策略：

(1) 热存储：用于存储近期（如1年内）影像数据，应采

用全闪存阵列或 SSD/SAS/SATA 混合阵列；

（2）温存储：用于存储中长期（如1至3年）影像数据，宜采用大容量NL-SAS/SATA磁盘阵列；

（3）冷存储：用于长期（3年以上）影像数据归档，宜采用磁带库、虚拟带库或蓝光光盘库等低成本、高持久性介质。

### （三）网络设备<sup>10</sup>

#### 1.核心交换机

（1）架构：采用模块化设计，主控、交换网板、电源、风扇等关键部件应支持冗余和热插拔；

（2）性能：整机交换容量、包转发率不低于当前主流核心交换机产品配置参数；

（3）端口：支持高密度的10Gb/25Gb/40Gb/100Gb自适应接口，满足不同速率接入需求；

（4）功能：支持VLAN、VXLAN、EVPN、STP、OSPF、BGP、SRV6等二、三层网络协议，并支持高可用、M-LAG或等效跨设备链路聚合技术以及Telemetry/IPCA遥测能力。

#### 2.汇聚交换机

（1）性能：整机交换容量、包转发率不低于当前主流汇聚交换机产品配置参数；

（2）端口：提供高密度的千兆和万兆光/电接口，上行接口

<sup>10</sup> 各省可根据实际情况，在满足需求的情况下上调要求。

速率不低于40Gbps;

(3) 功能: 支持VLAN、VXLAN、EVPN、STP、OSPF、BGP、SRV6等二、三层网络协议, 并支持高可用、M-LAG或等效跨设备链路聚合技术以及Telemetry/IPCA遥测能力;

(4) 可靠性: 关键部件如电源、风扇支持冗余和热插拔。

### 3.接入交换机

(1) 性能: 整机交换容量、包转发率不低于当前主流接入交换机产品配置参数;

(2) 端口: 下行提供不少于24个100/1000Mbps自适应电口; 上行提供不少于4个10Gb SFP+光口;

(3) 功能: 支持二层基础协议, VLAN、STP、链路聚合(LACP)、端口安全、ACL等二层安全与管理特性;

(4) 电源: 宜采用冗余可插拔电源模块, 提升设备可靠性。

### 4.广域网路由器

(1) 架构: 采用支持双主控、双电源等冗余设计的模块化路由器;

(2) 性能: 包转发性能应能满足专网和互联网出口总带宽的线速转发需求;

(3) 功能: 支持广域网络接入, 动态路由协议(OSPF/BGP/IS-IS), 支持NAT、QoS、VPN加密隧道、链路质量探测及智能路径调优、调度等功能;

(4)安全:支持主流安全加密传输技术、访问控制列表(ACL)等基础安全功能。

## 五、基础平台要求

### (一)服务器虚拟化

- 1.具备虚拟化集群管理、虚拟机在线迁移、克隆等核心功能;
- 2.具备宿主机故障时,虚拟机自动重启或迁移的高可用性(HA)功能;
- 3.宜具备分布式资源调度能力,实现计算资源的动态负载均衡;
- 4.宜支持网络虚拟化,实现灵活的网络策略定义和微分段。

### (二)存储虚拟化

- 1.采用分布式架构,实现单节点故障不影响数据存储的完整性和业务连续性;
- 2.支持统一提供块、文件、对象等多种存储服务类型。

## 六、云服务要求

若采用私有云或政务云服务,其提供的服务能力应不低于本规范中对私有化部署相应要求。

建议在采用云服务器GPU加速型等算力服务时,支持多品牌CPU/GPU及国产加速器等异构算力资源的统一池化管理与调度,并推动关键算法服务调用接口标准化。

### (一)云服务器

支持提供通用型、计算优化型、内存优化型、存储优化型、

GPU 加速型等多种实例规格。

## **(二) 云存储**

1.类型：支持提供块存储、文件存储、对象存储等多种存储类型；

2.对象存储可用性：服务可用性不低于99.99%，数据持久性不低于99.999999%；

3.静态数据加密：云存储服务宜启用静态数据加密功能。

## **(三) 云备份服务**

1.提供对云服务器、云硬盘等资源的快照或备份服务；

2.支持按策略自动执行备份任务，并能将数据恢复到任意备份点。

## **(四) 集中监控管理**

建设集中统一的监控平台，对所有服务器、网络设备、存储设备、基础软件及机房环境的核心运行指标（如CPU使用率、内存占用、网络流量、磁盘I/O、应用响应时间、温度）进行7×24小时不间断监控和历史数据分析，并建立分级告警机制与通知流程。

## **(五) 云安全服务**

云平台安全建设须满足GB/T 31168-2014《信息安全技术 云计算服务安全能力要求》要求。

# **七、网络要求**

## **(一) 总体建设要求**

- 1.影像云索引数据通过医疗保障核心业务区网络上传至国家医保信息平台；
- 2.各省医保影像云、定点医疗机构影像检查数据传输应通过新建的医保影像云专网；
- 3.医疗保障核心业务区网络与医保影像云专网应实现逻辑隔离；
- 4.网络架构设计需全面支持 IPv6 协议，同时具备双栈（IPv6/IPv4）接入与服务能力。

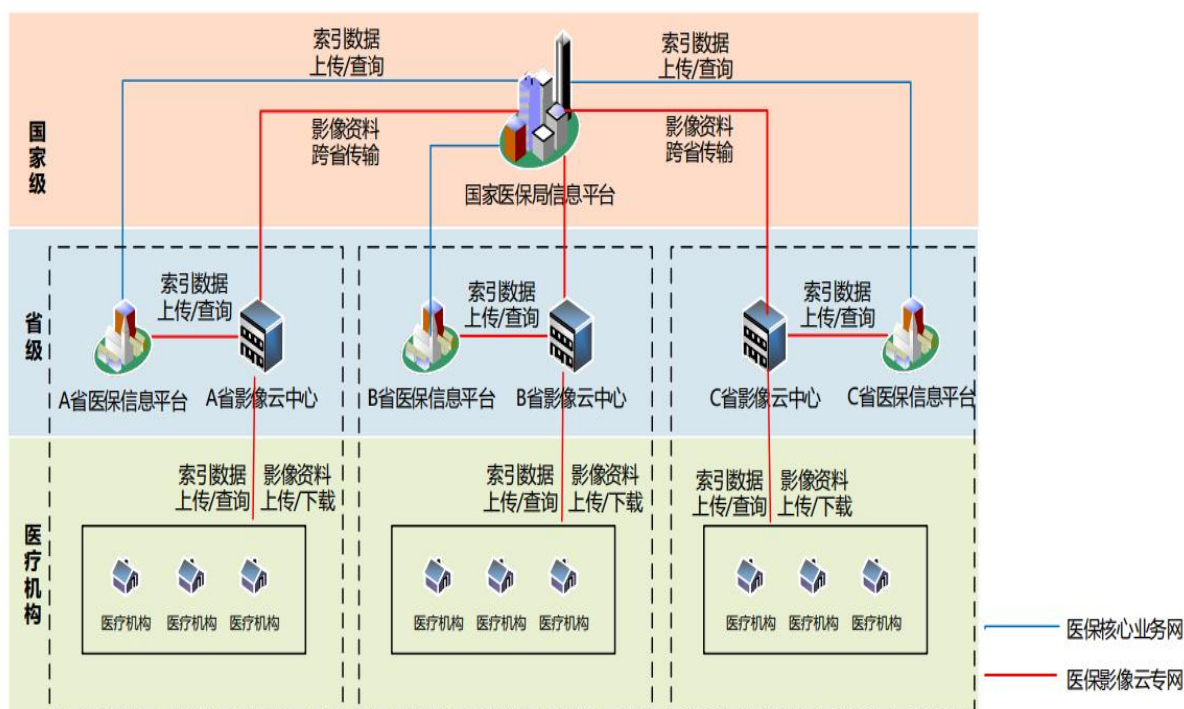


图 14 医保影像云专网组网示意图

## (二) 医保影像云专网

### 1.网络接入

各省医保影像云应依据《全国医疗保障系统核心业务区骨干

网络建设指南》（医保网信办〔2019〕3号）和《医疗保障核心业务区网络安全接入规范》（医保网信办〔2019〕40号），完成医保影像云专网安全、合规接入。

各省日均异地就诊转入或转出量超过2万人次时，应部署主备冗余线路。

## 2.性能指标

- （1）网络平均延迟  $\leq 100\text{ms}$ ;
- （2）平均丢包率  $\leq 0.1\%$ ;
- （3）全年网络可用性  $\geq 99.99\%$ 。

## 3.专线带宽

各省医保影像云应依据日均异地就诊转入和转出人口数量中的较高值，参考下表进行专线带宽基线选型，具体可结合实际情况上调。

表 1 医保影像云专线带宽要求对照表

日均异地就诊转入/转出人数	最低网络带宽要求 (Mbps)
$\geq 100000$	$\geq 4200$
$\geq 80000$	$\geq 3300$
$\geq 50000$	$\geq 2100$
$\geq 30000$	$\geq 1200$
$\geq 10000$	$\geq 400$
$\geq 5000$	$\geq 200$
$\geq 2000$	$\geq 100$

注：表中未列出数值，可参照已有数据按比例进行估算。

### (三) 定点医疗机构网络

#### 1. 性能指标

(1) 定点医疗机构接入医保影像云专线网络，其性能指标应符合专线带宽要求；

(2) 全年网络可用性  $\geq 99.95\%$ 。

#### 2. 专线带宽

定点医疗机构应依据日均影像数据上传量（参照表2）和日均院内就诊量（参照表3），分别估算上行与下行带宽需求，并按两者中的较高值进行专线带宽选型，具体可结合实际情况上调。

表 2 定点医疗机构专线上行带宽要求对照表

日均影像数据量	最低上行网络带宽要求 (Mbps)
$\geq 1000\text{GB}$	$\geq 900$
$\geq 800\text{GB}$	$\geq 700$
$\geq 500\text{GB}$	$\geq 450$
$\geq 300\text{GB}$	$\geq 250$
$\geq 200\text{GB}$	$\geq 200$
$\geq 100\text{GB}$	$\geq 100$
$\geq 50\text{GB}$	$\geq 50$

注：表中未列出数值，可参照已有数据按比例进行估算。

表 3 定点医疗机构专线下行带宽要求对照表

日均就诊量 (人次)	最低下行网络带宽要求 (Mbps)
$\geq 60000$	$\geq 2500$
$\geq 50000$	$\geq 2100$

≥30000	≥1200
≥10000	≥400
≥5000	≥200
≥2000	≥100
≥1000	≥50
≥500	≥20

注：表中未列出数值，可参照已有数据按比例进行估算。

#### （四）医保影像云互联网

各省医保影像云应根据本省日均检查量评估互联网带宽需求，并参照下表进行互联网带宽选型。互联网出口宜采用 BGP 多线方案，以提升访问质量和可用性。

表 4 医保影像云互联网带宽要求对照表

日均检查量（人次）	最低网络带宽要求（Mbps）
≥100000	≥2100
≥80000	≥1650
≥50000	≥1050
≥30000	≥600
≥10000	≥200
≥5000	≥100

注：表中未列出数值，可参照已有数据按比例进行估算。

### 八、安全防护要求

#### （一）医保影像云数据中心安全

1.网络防火墙：应在数据中心网络边界、互联网出口及内部

核心区域边界部署高性能网络防火墙，用于访问控制、安全区域隔离及网络威胁防护。

**2.入侵防御系统：**具备对各类网络攻击行为进行深度检测、实时行为分析与主动阻断防御。

**3.Web 应用防火墙：**具备对 SQL 注入、跨站脚本（XSS）、文件上传漏洞等常见 Web 攻击的防护能力。

**4.日志审计系统：**能够对网络设备、安全设备、服务器、操作系统、数据库和应用等所有 IT 组件的日志进行集中采集、范式化、关联分析和安全存储。日志保存时间应不少于 180 天。

**5.数据库审计系统：**对数据库的访问操作进行独立监控、记录和分析，并对 SQL 注入、越权访问等高危操作进行实时告警。

**6.运维审计系统：**对所有运维人员（内部员工、外部合作方）的远程访问进行统一身份认证、权限控制、操作审计和会话录像回放。

**7.漏洞扫描设备：**具备对主机、网络设备、Web 应用、数据库等资产进行定期自动化漏洞扫描能力，并提供修复建议和风险趋势报告。

**8.态势感知与综合安全管理平台：**宜部署态势感知与综合安全管理平台，联动整合、统一管理各类安全设备，对各类安全日志和事件进行集中关联分析，整合威胁情报，实现威胁的统一监测、预警、研判和响应处置。

**9.数据防泄漏系统：**宜在网络出口和终端，部署数据防泄漏系统，对包含个人身份信息、影像诊断报告等敏感数据的外发行为进行深度内容检测、监控和阻断。

## **10.传输安全**

(1) 业务系统之间涉及敏感数据传输时，须采用基于国密算法或 TLS1.2 及以上协议的安全加密套件，严禁使用包含弱算法或特性的套件，关键业务系统<sup>11</sup>优先推荐选用国密算法套件；

(2) 个人敏感信息除通过安全传输通道传输外，须根据业务安全需求对敏感字段及敏感数据内容采取加密保护措施；

(3) 互联网区需要具备防护 DDOS 攻击能力。

### **(二) 网络边界与通信安全**

**1.网络隔离：**通过部署网络防火墙或安全隔离网闸，实现不同安全等级网络区域（如互联网接入区、应用服务区、数据核心区、运维管理区）之间的有效隔离和访问控制。

**2.流量控制：**宜部署流量控制设备，对网络流量进行分析和管控、告警，具备用户行为分析、应用带宽限制、应用带宽保障、链路监测、自动告警等功能。

### **(三) 终端安全**

**1.终端认证：**终端接入系统时，应采用至少两种组合鉴别技

<sup>11</sup> 规范中仅明确基础要求，具体“关键业务系统”与“关键业务数据”以各省实际情况自行定义。

术（如密码+短信验证码、密码+数字证书）进行身份认证，即多因素认证。

**2.传输加密：**终端设备通过公共网络访问业务系统时，须采用基于国密算法或 TLS1.2 及以上协议对传输数据进行加密保护，关键业务系统推荐选用国密算法进行加密。

**3.终端防护：**所有接入网络的终端（包括服务器和个人电脑）应安装统一管理的防病毒软件，并宜具备终端侦测与响应能力。

**4.密钥管理安全：**应建立完善的密钥全生命周期管理体系，包括密钥生成、分发、存储、轮换和销毁。核心数据加密，宜采用经过国家密码管理部门认证的硬件加密机进行密钥安全保管。

#### **（四）身份与访问管理**

**1.统一身份认证：**应建立集中式身份管理系统，对所有用户（内部员工、外部合作方）和系统账号进行统一生命周期管理（创建、授权、禁用、删除）。

**2.多因素认证：**所有对生产环境访问，尤其是涉及特权账号访问（如服务器 SSH、数据库登录、云平台控制台），应强制启用多因素认证。

**3.权限访问控制：**应严格遵循“最小权限”和“职责分离”原则，实施基于角色的访问控制，确保每个用户仅拥有其完成本职工作所必需的最小权限集合，并定期（如每半年）对用户权限进行审查。

## （五）安全运营与审计

**1.定期安全评估：**应定期（至少每年一次）委托具备资质的第三方机构开展渗透测试和安全评估，从攻击者视角检验系统实际安全防护能力，并对发现风险进行跟踪修复。

**2.应急响应：**应建立正式的安全事件应急响应预案和保障团队，明确事件上报、研判、处置、溯源和恢复流程。宜定期组织应急响应演练，确保预案可行性和团队熟练度。

**3.配置与补丁管理：**应建立正式的流程和工具，对所有 IT 资产的安全配置基线进行统一管理和合规性检查，并对机构发布的高危安全补丁进行评估、测试和及时部署。

## 九、容灾备份要求

### （一）容灾目标

**1.恢复时间目标（RTO）：**关键业务系统 RTO 不超过 4 小时。

**2.恢复点目标（RPO）<sup>12</sup>：**关键业务数据 RPO 不超过 1 小时。

### （二）数据备份

医保影像云应对核心业务数据和系统配置进行定期、自动化本地备份，可采用数据快照、同/异步复制等技术。

## 十、存储介质处置要求

存储个人敏感信息或重要业务数据的介质在报废、维修或转

<sup>12</sup> 具体时长以各省实际情况自行定义。

让前，应通过不可逆的数据擦除（如多次覆写）或物理销毁（如消磁、粉碎）方式，确保其存储的数据无法被任何技术手段恢复。

# 医保影像云—业务人员、设备及图像基础要求

## 一、适用范围

本规范明确医保影像云业务涉及的人员资质、设备管理、图像基础要求，适用主体为各级医保部门、定点医疗机构及第三方技术服务机构开展的医保影像云相关业务活动。

## 二、定义

**(一) DICOM 元数据:** 遵循 DICOM (数字医学影像通信标准) 格式, 包含患者标识 (姓名、ID 号等)、扫描参数 (层厚、螺距、管电压等) 等图像相关信息的数据集合。

**(二) X 线设备:** 利用 X 射线穿透人体组织, 通过测量透过人体的 X 线强度差异形成影像, 用于疾病诊断的医学影像设备。

**(三) CT 设备:** 利用 X 射线对人体进行扫描, 通过探测器采集多角度 X 线衰减数据, 借助计算机重建技术获得人体某一层面 (横断面) 组织结构影像的设备。

**(四) MRI 设备:** 利用人体内氢原子核在静磁场中受射频脉冲激励产生 MRI 信号, 通过梯度磁场空间定位, 经计算机处理重建出人体组织形态和功能影像的非电离辐射式医学成像设备。

## 三、业务人员要求

人员从业管理应当遵循《中华人民共和国医师法》及卫生健

康主管部门的相关规定，应通过辐射安全防护培训，取得《放射人员工作许可证》。其中，独立从事医学影像诊断工作的，应取得《医师资格证书》，并经执业注册取得对应《医师执业证书》，同时应取得国家医保医师代码。

#### **四、医学影像设备要求**

医学影像设备需满足国家及地方卫生健康行政部门关于设备配置规划、使用规范、质量管理的各项要求，应取得医保医用设备（成像类）代码，并具备相应设备配置许可证等；其中大型医学影像设备需按规定进行年检，确保设备运行稳定性。

##### **（一）三级医疗机构建议**

1.X线设备：建议配备500mA以上（含500mA）高频X线平板探测器设备、移动式X线设备、多功能X线设备（数字胃肠机）、钼靶X线乳腺成像设备等；

2.CT设备：建议配备64层以上（含64层）螺旋CT设备；

3.MRI设备：建议配备3.0T以上（含3.0T）科学研究型MRI设备。

##### **（二）二级医疗机构建议**

1.X线设备：建议配备500mA以上（含500mA）高频X线平板探测器设备、移动式X线设备、多功能X线设备（数字胃肠机）、钼靶X线乳腺成像设备等；

2.CT设备：建议配备16层以上（含16层）螺旋CT设备；

3.MRI 设备：建议配备临床实用型 MRI，根据医院情况配置合适的场强。

### **（三）基层医疗机构建议**

X 线设备：建议配备 500mA 以上（含 500mA）高频 X 线平板探测器设备。

## **五、影像检查图像基础要求**

**（一）有效图像：**影像检查图像应确保清晰度与可辨识度，能够为诊断提供准确依据，严禁出现全黑、全白等无效影像。

**（二）真实人体图像：**影像检查图像须真实反映人体解剖结构，严禁使用非真实人体图像，如仿人体模型、质控水模、动植物等。

**（三）原始完整图像：**原始完整图像包含影像设备直接采集的图像和为满足临床诊断生成的后处理图像（如三维重建、全脊柱拼接等）；严禁篡改 DICOM 标签信息，严禁对图像实施非诊断必要的添加、删减、像素篡改及伪造等违规操作。

**（四）非拼接图像：**影像检查图像须完整包含患者同一次检查的全部图像，严禁将不同机构、不同患者、不同时间采集的检查图像拼接为同一次影像检查图像。

**（五）非重复图像：**患者影像检查图像不得重复归集至不同检查记录，严禁任何影像检查图像跨患者、跨机构重复归集与上传。

**(六) 患者信息相符：**影像检查图像特征须与患者年龄、性别、病史等信息相符。

**(七) 检查部位一致：**影像检查图像显示的检查部位须与检查报告、医保结算对应信息保持一致。