ICS 35.240.80
CCS L77

T/ZPP

团 体 标 准

T/ZPP XXXX—2025

远程医疗多中心会诊数据交互规范

Telemedicine multi-center consultation data exchange standard

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

2025－XX－XX 发布　　2025－XX－XX 实施

浙江省品牌建设促进会　　发 布

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××××提出。

本文件由××××归口。

本文件起草单位：

本文件主要起草人：

远程医疗多中心会诊数据交互规范

1 范围

本文件规定了远程医疗多中心会诊数据交互的总体要求、系统架构、数据内容与格式、数据交互流程、安全与隐私保护及运维管理等核心内容，明确了多中心会诊过程中数据采集、传输、共享、存储的全流程标准。

本文件适用于开展远程医疗多中心会诊的医疗机构、第三方医疗服务平台、医疗数据技术提供商等相关主体，覆盖综合会诊、专科会诊、病例讨论等多类型远程医疗场景。

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/T 35273 信息安全技术 个人信息安全规范

GB/T 39786 信息安全技术 信息系统密码应用基本要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

远程医疗多中心会诊 telemedicine multi-center consultation

由一家牵头医疗机构联合两家及以上参与医疗机构，依托远程医疗信息系统，围绕同一患者的病情诊断、治疗方案制定等开展的跨机构、协同性医疗服务活动。

3.2

数据交互 data exchange

在远程医疗多中心会诊全流程中，各参与方之间进行患者临床数据、影像数据、检验检查结果、会诊意见等数据的采集、传输、共享、接收与反馈的过程。

3.3

牵头医疗机构 leading medical institution

发起远程医疗多中心会诊，负责组织协调、数据汇总、会诊主持及最终意见整合的医疗机构。

3.4

参与医疗机构 participating medical institution

受牵头医疗机构邀请，提供专业医疗意见、共享相关医疗数据，参与会诊讨论的医疗机构。

3.5

医疗数据元 medical data element

构成医疗数据的基本单位，包括患者基本信息、临床诊断、检验检查结果等数据的最小标识单元，符合 WS 363—2011 要求。

3.6

数据交互接口 data exchange interface

实现不同远程医疗系统间数据互联互通的标准化技术接口，包括API接口、消息队列接口等。

3.7

数据脱敏 data desensitization

通过屏蔽、替换、加密等技术手段，对患者个人敏感信息进行处理，确保数据在交互过程中不泄露个人隐私的技术过程，符合GB/T 35273要求。

3.8

数据完整性 data integrity

会诊数据在采集、传输、存储过程中保持完整、未被篡改、未丢失的特性。

3.9

会诊数据集市 consultation data mart

专门用于存储、管理多中心会诊相关数据的集中式数据存储单元，支持数据快速检索与共享。

4 总体要求

4.1 核心原则

4.1.1 合规性原则

数据交互全过程应严格遵守《数据安全法》《个人信息保护法》等法律法规及相关标准要求，确保数据采集、传输、共享、存储等环节合法合规，患者隐私得到充分保护。

4.1.2 标准化原则

数据内容、格式、接口协议、交互流程应遵循统一标准，确保不同医疗机构、不同系统间的数据互联互通，消除数据孤岛。

4.1.3 安全性原则

建立全流程数据安全防护体系，保障数据在交互过程中的保密性、完整性、可用性，防范数据泄露、篡改、丢失等安全风险。

4.1.4 实用性原则

数据交互流程应简洁高效，数据内容应精准实用，满足多中心会诊的临床需求，避免冗余数据传输，提升会诊效率。

4.1.5 可追溯性原则

会诊数据交互的每一个环节都应留有记录，包括数据来源、传输时间、处理人员、交互结果等，实现数据全生命周期可追溯。

4.1.6 扩展性原则

系统架构与数据交互机制应具备良好的扩展性，能够适配未来医疗技术发展、会诊业务拓展及数据类型增加的需求。

4.2 核心指标要求

4.2.1 数据质量指标

数据质量指标如下：

a) 数据完整性：核心数据元完整率≥99%，非核心数据元完整率≥95%；
b) 数据准确性：患者身份标识匹配准确率 100%，临床数据录入错误率≤0.5%；
c) 数据一致性：同一患者相同数据在不同机构间的一致性≥99%；
d) 数据时效性：检验检查数据、影像数据传输时延≤30 分钟，会诊意见反馈时延≤2 小时。

4.2.2 系统性能指标

系统性能指标要求如下：

a) 接口响应时间：单次数据查询与传输响应时间≤3 秒；
b) 并发处理能力：支持同时在线会诊≥50 场，单场会诊参与机构≥10 家；
c) 系统可用性：全年系统可用率≥99.9%，故障恢复时间≤4 小时；
d) 数据传输成功率：各类会诊数据传输成功率≥99.5%。

4.2.3 安全防护指标

安全防护指标如下：

a) 数据加密率：敏感数据加密存储与传输率 100%；
b) 访问控制准确率：用户权限访问控制准确率 100%；
c) 安全审计覆盖率：数据交互全流程安全审计覆盖率 100%；
d) 漏洞修复及时率：高危安全漏洞修复及时率 100%，中危漏洞修复及时率≥95%。

5 系统架构

5.1 架构设计原则

5.1.1 分层架构

采用“数据层-服务层-应用层”三层架构设计，各层级职责清晰、松耦合，支持独立升级与扩展。

5.1.2 分布式部署

支持牵头医疗机构、参与医疗机构分布式部署，通过标准化接口实现数据实时交互与同步。

5.1.3 安全嵌入

将安全防护机制嵌入各层级，实现从数据采集到存储的全流程安全管控。

5.1.4 兼容适配

兼容现有主流医院信息系统（HIS）、临床信息系统（CIS）、医学影像存档与通信系统（PACS）、实验室信息系统（LIS）等医疗信息系统。

5.2 架构组成

5.2.1 数据层

5.2.1.1 数据存储模块：包括会诊数据集市、患者数据缓存、历史会诊档案库，支持结构化数据（如检验结果）、非结构化数据（如影像文件、病历文档）的存储。
5.2.1.2 数据治理模块：负责数据清洗、脱敏、标准化转换、质量校验，确保数据符合交互要求。
5.2.1.3 数据备份模块：采用“本地备份+异地容灾”模式，定期进行数据备份，备份频率≥1 次/天，备份数据保留期限≥3 年。

5.2.2 服务层

5.2.2.1 接口服务模块：提供标准化 API 接口、消息队列接口、文件传输接口，支持数据的查询、上传、下载、推送等操作。
5.2.2.2 数据交互服务模块：负责数据路由、传输调度、交互协议转换，确保数据在不同系统间高效传输。
5.2.2.3 安全服务模块：提供身份认证、权限管理、数据加密、安全审计等安全服务。
5.2.2.4 业务逻辑服务模块：实现会诊发起、邀请、数据汇总、意见整合等业务逻辑处理。

5.2.3 应用层

5.2.3.1 会诊管理模块：支持会诊发起、参与机构邀请、会诊时间预约、会诊状态跟踪等功能。
5.2.3.2 数据交互模块：提供数据上传、下载、查询、共享、反馈等操作入口。
5.2.3.3 会诊协作模块：支持多机构实时沟通、影像共同阅片、病例讨论等协作功能。
5.2.3.4 报表统计模块：支持会诊数据、交互数据、质量指标等的统计与分析。

5.3 接口架构

5.3.1 接口类型

接口类型如下：

a) 数据查询接口：支持牵头医疗机构查询参与机构的相关医疗数据，采用 RESTful API 设计；
b) 数据上传接口：支持参与机构向牵头机构上传会诊所需数据，支持批量上传与断点续传；

c) 数据推送接口：支持系统间实时推送会诊通知、数据更新、意见反馈等信息，采用消息队列机制；
d) 文件传输接口：用于传输影像文件、大型病历文档等，支持加密传输与校验。

5.3.2 接口协议要求

接口协议要求如下：
a) 传输协议：采用 HTTPS 协议进行数据传输，文件传输可采用 SFTP 协议；
b) 数据交换格式：采用 JSON 格式传输结构化数据，XML 格式传输复杂业务数据；
c) 接口版本控制：支持接口版本管理，版本升级需保持向下兼容；
d) 接口文档：提供完整的接口文档，包括接口地址、参数说明、返回值说明、错误码定义等。

6 数据内容与格式

远程医疗多中心会诊交互数据分为6大类，具体内容见表1。

表 1 会诊交互数据分类及核心内容表

数据类别	核心数据元	数据来源	必选/可选
患者基本信息	患者唯一标识、姓名（脱敏）、性别、年龄、联系方式(脱敏)、民族、籍贯	牵头医疗机构HIS系统	必选
临床诊断信息	主诉、现病史、既往史、个人史、家族史、体格检查结果、初步诊断、诊断依据	牵头医疗机构CIS系统	必选
检验检查信息	检验项目名称、检验结果、参考范围、检验时间、检验机构；检查项目名称、检查结论、检查图像、检查时间、检查机构	牵头/参与医疗机构 LIS/PACS系统	必选
影像数据	医学影像文件（DICOM格式）、影像报告、影像标注信息	牵头/参与医疗机构PACS系统	按需必选
治疗相关信息	已采取的治疗措施、用药史、手术史、疗效评价	牵头医疗机构CIS系统	可选
会诊相关信息	会诊申请单、参与专家信息、会诊意见、会诊结论、后续治疗建议	牵头/参与医疗机构会诊系统	必选

7 数据交互流程

7.1 总体流程

远程医疗多中心会诊数据交互流程分为会诊准备阶段、会诊实施阶段、会诊总结阶段三个阶段，各阶段有序衔接，确保数据高效流转。

7.2 会诊准备阶段数据交互流程

流程如下：
a) 会诊发起：牵头医疗机构通过会诊系统发起多中心会诊申请，录入患者基本信息、初步诊断、会诊需求等数据，系统自动生成唯一会诊编号；
b) 机构邀请：牵头医疗机构通过系统向参与医疗机构发送会诊邀请，邀请信息包括会诊编号、患者基本信息（脱敏）、会诊时间、会诊需求、所需数据清单；
c) 响应邀请：参与医疗机构接收邀请后，在 24 小时内反馈是否参与会诊；同意参与的，确认可提供的数据类型与范围；
d) 数据采集：牵头医疗机构采集本机构内患者的临床诊断、检验检查、影像等数据，进行标准化处理与脱敏；

e) 数据请求：牵头医疗机构通过标准化接口向参与医疗机构发送数据查询请求，明确所需数据内容；
f) 数据提供：参与医疗机构接收数据请求后，验证请求合法性，提取相关数据并进行脱敏、标准化转换，在会诊前 48 小时内通过接口上传至牵头医疗机构；
g) 数据汇总：牵头医疗机构接收各参与机构的数据，进行数据质量校验与整合，形成完整的会诊病例数据包，供会诊时使用。

7.3 会诊实施阶段数据交互流程

流程如下：
a) 数据共享：会诊开始后，牵头医疗机构通过会诊系统向所有参与机构共享整合后的病例数据包，支持多机构同时查看；
b) 实时交互：会诊过程中，参与机构可通过系统上传补充数据、发表初步意见，数据实时同步至所有参与方；
c) 影像交互：支持多机构对影像数据进行共同阅片、标注、测量，标注信息实时同步；
d) 意见反馈：参与专家通过系统提交阶段性会诊意见，意见实时推送至牵头医疗机构及其他参与机构；
e) 数据查询：会诊过程中，各机构可根据需要查询相关补充数据，系统实时响应查询请求。

7.4 会诊总结阶段数据交互流程

流程如下：
a) 意见汇总：会诊结束后，牵头医疗机构汇总所有参与机构的会诊意见，形成最终会诊结论与治疗建议；
b) 数据反馈：牵头医疗机构通过接口将最终会诊报告推送至各参与医疗机构及患者就诊机构；
c) 数据归档：牵头医疗机构将完整的会诊数据（包括申请单、病例数据、会诊意见、会诊报告）进行归档存储，归档数据保留期限≥3 年；
d) 数据同步：参与医疗机构将会诊报告同步至本机构的医疗信息系统，纳入患者病历档案。

7.5 异常处理流程

流程如下：
a) 数据传输失败：当数据传输失败时，系统自动重试（重试次数≤3 次）；重试失败的，向发起方发送失败通知，发起方可手动重新发起数据传输；
b) 数据质量异常：接收方发现数据缺失、错误等质量问题时，向发送方发送数据修正通知，发送方在 12 小时内修正并重新上传；
c) 系统故障：若系统出现故障，暂停数据交互，故障修复后，恢复数据交互流程，确保数据连续性；
d) 权限异常：当出现权限访问异常时，系统自动记录并报警，管理员及时核查处理，确保数据访问安全。

8 安全与隐私保护

8.1 身份认证与访问控制

8.1.1 身份认证

采用“用户名+密码+动态验证码”或数字证书的双因素认证方式，确保用户身份真实性；远程访问需额外进行IP绑定、设备认证，限制未授权设备访问；认证失败次数累计≥5次时，锁定账号1小时，防止暴力破解。

8.1.2 访问控制

基于角色的访问控制（RBAC）模型，划分牵头机构管理员、参与机构管理员、会诊专家、普通操作员等角色，明确各角色的数据访问权限；实现数据访问的最小权限原则，用户仅能访问其职责所需的数据；支持细粒度权限控制，可按数据类别、患者范围设置访问权限。

8.2 数据加密

8.2.1 传输加密

所有数据传输采用HTTPS协议，加密算法采用TLS 1.3标准；影像文件、大型文档传输采用AES-256 加密算法；接口调用采用API密钥+签名机制，确保传输数据不被篡改。

8.2.2 存储加密

敏感数据存储采用AES-256加密算法，加密密钥定期更换（更换周期≤90天）；患者身份标识采用不可逆加密处理，确保隐私安全；加密密钥采用专人管理、分级存储，防止密钥泄露。

8.3 数据脱敏与隐私保护

8.3.1 数据脱敏

数据交互过程中，对患者身份证号、手机号、详细地址等敏感信息进行脱敏处理，脱敏处理不影响临床使用；会诊结束后，非必要保留的敏感数据应进一步脱敏或删除；脱敏规则统一、透明，确保多中心脱敏标准一致。

8.3.2 隐私保护

严格遵守《个人信息保护法》要求，采集患者数据前需获得患者或其监护人的明示同意，明确告知数据使用范围与目的；禁止将会诊数据用于非医疗目的，禁止向无关第三方泄露；涉及未成年人、传染病患者等特殊人群的数据，采取额外隐私保护措施。

8.4 安全审计与追溯

建立全面的安全审计机制，记录所有数据交互操作，包括用户登录、数据查询、上传、下载、修改、删除等操作；审计日志包含操作人、操作时间、操作内容、操作结果、IP地址、设备信息等要素，日志保留期限≥1年；支持审计日志的查询、导出、分析，便于安全事件追溯与责任认定。

8.5 数据出境管理

会诊数据原则上不得出境；确需出境的，应按照GB/T 39786要求开展数据出境安全评估，评估通过后方可出境；出境数据需进行严格脱敏处理，确保不包含敏感个人信息与重要医疗数据；建立数据出境台账，记录出境数据内容、接收方、出境目的、安全措施等信息。

9 运维管理

9.1 日常运维

9.1.1 运维职责

运维职责如下：

a) 运维单位负责系统的日常运行监控、故障处理、性能优化、安全维护；
b) 建立 7×24 小时值班制度，实时监控系统运行状态，及时发现并处理异常；
c) 定期检查数据存储设备、网络设备、安全设备的运行状态，确保设备正常工作。

9.1.2 运维周期

运维周期如下：

a) 日常监控：实时监控系统 CPU、内存、磁盘空间、网络带宽等资源使用情况，监控频率≤5 分钟/次；
b) 定期巡检：每周开展 1 次系统全面巡检，包括功能、性能、安全等方面；
c) 数据备份检查：每月检查数据备份完整性与可恢复性，确保备份有效；

d) 安全扫描：每月开展 1 次系统安全扫描，每季度开展 1 次渗透测试。

9.2 故障管理

9.2.1 故障分级

故障分级应符合：

a) 一级故障（重大）：系统完全瘫痪，无法开展数据交互，影响多场会诊；
b) 二级故障（主要）：核心功能异常，部分数据交互无法进行，影响单场或少数会诊；
c) 三级故障（次要）：非核心功能异常，不影响核心数据交互；
d) 四级故障（轻微）：界面、操作等小问题，无影响数据交互。

9.2.2 响应时限

响应时限如下：

a) 一级故障：响应时间≤30 分钟，修复时间≤4 小时；
b) 二级故障：响应时间≤1 小时，修复时间≤8 小时；
c) 三级故障：响应时间≤2 小时，修复时间≤24 小时；
d) 四级故障：响应时间≤4 小时，修复时间≤48 小时。

9.2.3 故障处置

建立故障上报、登记、处理、反馈的闭环管理流程；故障修复后，24小时内进行复盘分析，查找故障原因，避免同类故障重复发生；重大故障修复后，向相关主管部门提交故障处置报告。

9.3 系统升级与更新

系统升级前需进行充分测试，确保升级后系统兼容原有功能与数据；升级计划提前7天通知各使用单位，选择非工作时间（如夜间、节假日）进行升级，减少对业务的影响；升级后提供升级说明文档，开展必要的培训，确保用户熟悉新功能；建立版本回滚机制，若升级后出现重大问题，可在2小时内回滚至原版本。

9.4 培训与支持

对使用单位的管理员、操作员开展专项培训，培训内容包括系统操作、数据交互流程、安全规范等；提供在线客服、电话支持等多种技术支持渠道，响应时间≤2小时；建立常见问题知识库，方便用户自行查询解决问题；每半年开展1次用户满意度调查，收集用户意见，持续优化系统与服务。