远程协诊项目
系统设计及接入计划

1、项目概要

1）简介

远程协诊系统是一套基于专网/安全互联网下的单病种远程协诊平台，通过在医院部署移动远程协诊系统，与医院信息系统对接，向医生提供移动客户服务端，实现中心医院与合作医院医生间直接的协作诊疗业务，完成学科内重大疾病远程指导、筛查、定位及转诊。

业务开展是在医生主动推送的前提下，将该患者临床信息和协作信息上传到数据中心，并通过数据中心接入云服务平台，协作医生利用碎片时间，通过移动客户服务端接受协诊请求，从云服务平台调取协作信息和临床信息，通过客户端完成与申请医生、患者的视频、语音或者电话互动沟通，给出意见。

合作医院的初诊病例中包括众多疑似重大疾病手术患者，而又不能独立完成的，通过协诊合作，对耗费精力再寻找优质医疗服务的患者人群，可精准定位并转诊到中心医院接受医疗服务,在完成特定医疗服务后，转诊回合作医院继续治疗。

2）特点

- 全景病例信息

移动远程协诊系统对接医院临床信息系统，在发送远程协诊申请时，基于医生的主管选择，系统将包括患者医嘱、病程、影像检查（包括原始 Dicom 影像图片）、检验以及实时动态生理指标信息等全临床信息上传数据中心服务器，协诊医生依据患者的全临床信息，并与合作医院医生、患者互动沟通作为判断依据。

- 规范业务流程

移动远程协诊系统紧密结合医疗业务规范操作要求,在业务发生的各个环节，严格遵循远程医疗业务规范，从协诊资格确认、协诊业务质量保障、医务部门监管以及医疗责任认定措施方面重重把关，支持可追溯的业务流监控。

- 互联网化体验

基于完整临床信息共享以及业务流程规范，移动远程协诊依托互联网化技术作为业务开展的载体。医生通过移动设备通过点选完成协诊申请的发送，协诊医生通过移动设备调取信息、开启互动、填写意见、签名确认并发回，基层医生直接打印协诊报告单存档。业务开展过程中，通过微信、短信等多种形式作为业务节点的提醒工具，使得医生不需要一直关注协诊业务。异步操作和移动体验，使得医生可以随时随地的完成协诊业务。

2、系统部署与实施

技术实施公司将派遣技术工程师到现场负责完成会诊系统的部署、数据对接、系统调试、培训等工作，并最终交付科室用户及操作员，能够自行完成会诊业务的全部操作。

序号	实施阶段	说明
1	设备发货与签收	专用移动会诊终端发货到医院，并由医院专职负责人签收。
2	服务器部署与调试	在院内部署会诊系统，调试系统，调试网络
3	系统对接	分别与医院 HIS,LIS,EMR,PACS 等系统实现数据对接，此过程需要医院及厂商强力配合，以实现数据对接的稳定性与可靠性
4	数据准备	在会诊平台上维护好医院、科室、医生基础信息
5	设备发放与培训	向参与会诊的科室交付会诊终端，并培训每位参与会诊的医生能够自主操作： 发起方：会诊申请、会诊信息选择与填写、会诊意见接收、会诊记录单的打印； 接收方：会诊通知、病历浏览、影像浏览处理、发送会诊意见、签名确认等。
6	系统试运行	每个科室用户自主收发一定量的会诊，确保系统平稳正常运行

7	技术维护	培训信息科专职人员维护会诊系统，能够解决一些常规的技术问题，并在出现问题时及时与公司联系远程解决。
8	系统交付	设备交付、技术文档交付，系统正常运行。

4、信息系统接口说明

详见《系统接口技术方案》

此方案为详尽的合作医院系统接入接口说明，由省医交由合作医院信息科，并协调完成与远程协诊系统的数据对接

5、安全设计说明方案

详见《系统安全设计方案》

此方案针对远程协诊平台的安全设计，系统架构、安全及数据安全，作以说明。

远程协诊项目
安全设计方案

1、 方案简介

1.1 业务架构

1）业务架构如图所示：

2）整个系统包括患者智能终端系统、合作医院与省医院内信息系统接入及部署、区域数据中心的部署以及云平台系统的部署。因此本方案将分别从云平台、区域数据中心到院内系统的接入与部署等几个方面进行安全设计。

3）医院与数据中心之间采用卫生专网或基于 VPN 通道连接。

4）同一区域数据中心下的各医院网络协作临床病历等数据封闭在同一局域网络内部，以保障其网络及数据安全性。

1.2 系统设计原则

通过对网络系统的风险分析及需要解决的安全问题，我们制定合理的安全策略及安全方案来确保网络系统的机密性、完整性、可用性、可控性与可审查性。

- 可用性： 授权实体有权访问数据 。
- 机密性： 信息不暴露给未授权机构或个人。
- 完整性： 保证数据不被未授权修改。
- 可控性： 控制授权范围内的信息流向及操作方式可审查性：对出现的安全问题提供依据与手段。

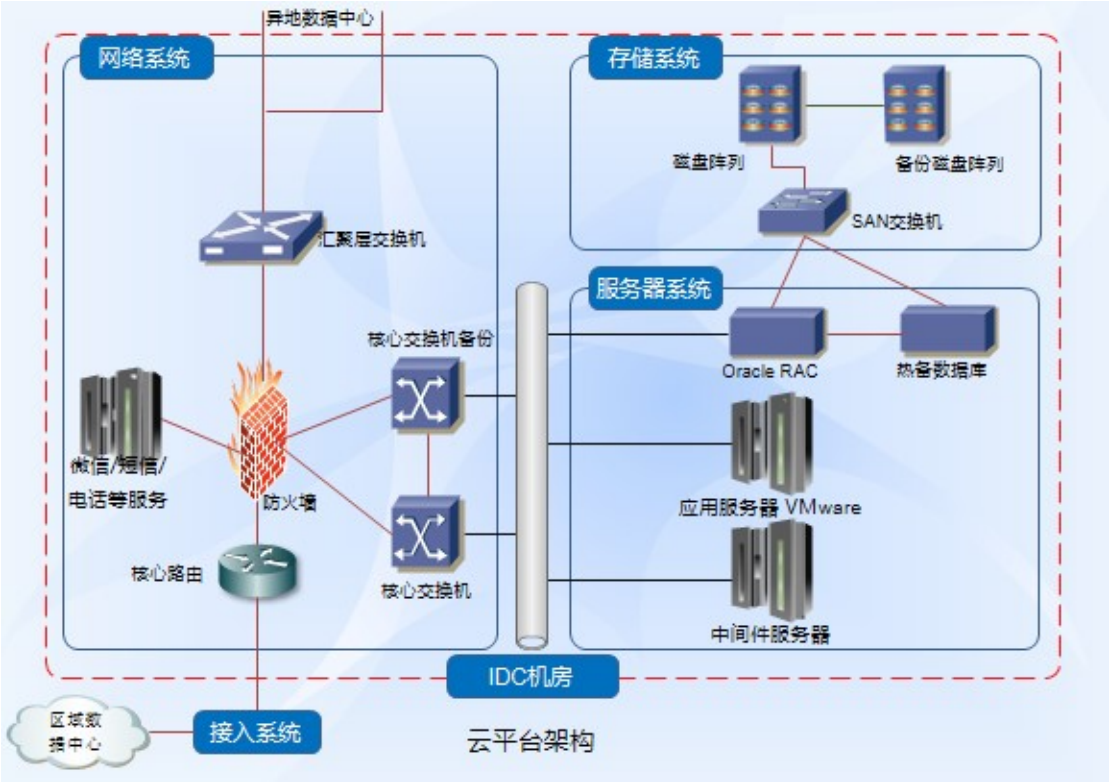
2、 云平台安全设计

2.1 云平台应用简介

云平台负责远程协诊系统的基础数据资源的协调，通过光纤接入，与区域数据中心网络相连。

整个云平台包括数据存储系统、主机服务器系统、网络安全系统等构成。其安全设计主要体现在网络系统的安全设计中。

2.2 云平台安全设计拓扑结构



2.3 网闸/防火墙规则安全

云服务器托管于省医中心机房，对外网络边界采用防火墙+网闸，系统决定了哪些内部服务可以被外界访问；外界的哪些服务可以访问内部的哪些服务，及

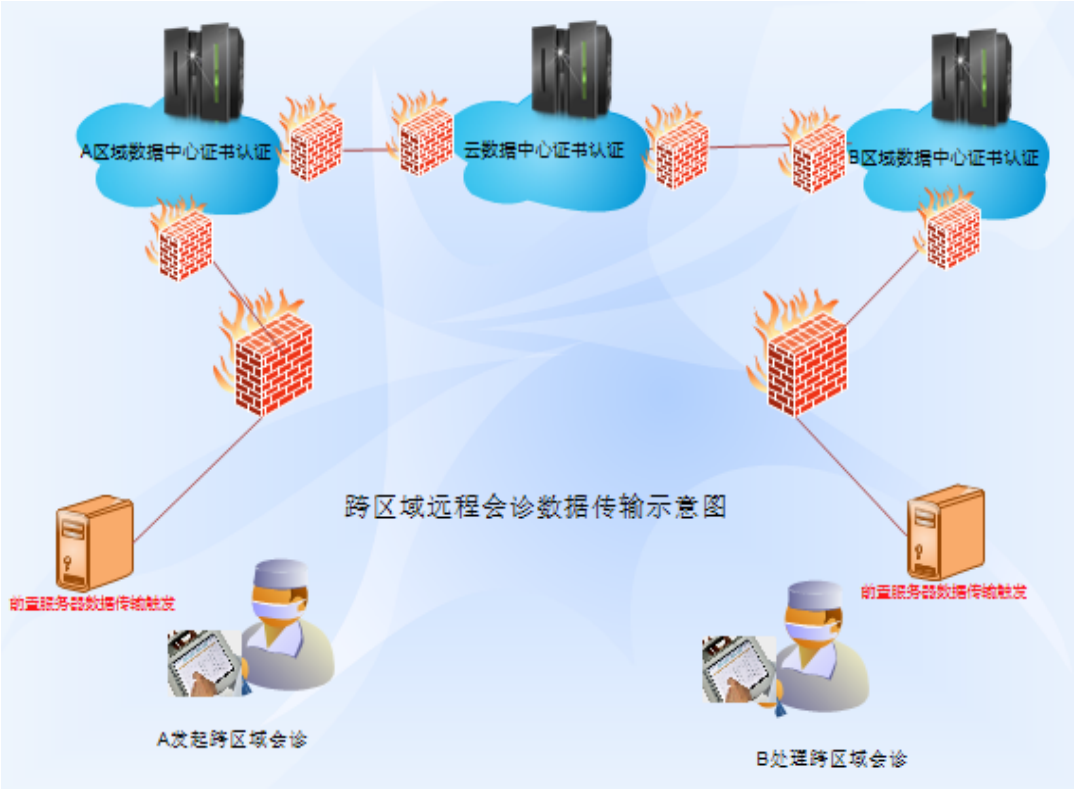
哪些外部服务可以被内部人员访问。所有来自和去往 Internet 的信息都必须经过防火墙，接受防火墙的检查。防火墙只允许授权的数据通过，并且防火墙本身也能够免于渗透。

- IP/MAC 地址的可信（类似于 DNA），生物身份。（区域数据中心服务器）
- 身份精细—MAC/用户的精确。（医疗机构前置服务器）
- 数据加密保护。
- 安全隔离。
- 设备安全

2.4 通迅安全

- 通讯采用与授信设备签名认证+证书认证+数据加密传输（非对称加密）。
- 云平台服务只被动转发授权区域数据中心；授权服务器；授权医生主动发出的需要其它区域专家会诊的医疗数据，而且云平台只保存记录；不保存这些数据，确保用户数据不被监听、篡改、丢失、被盗等等，避免造成医生与患者隐私信息泄露。

如图：



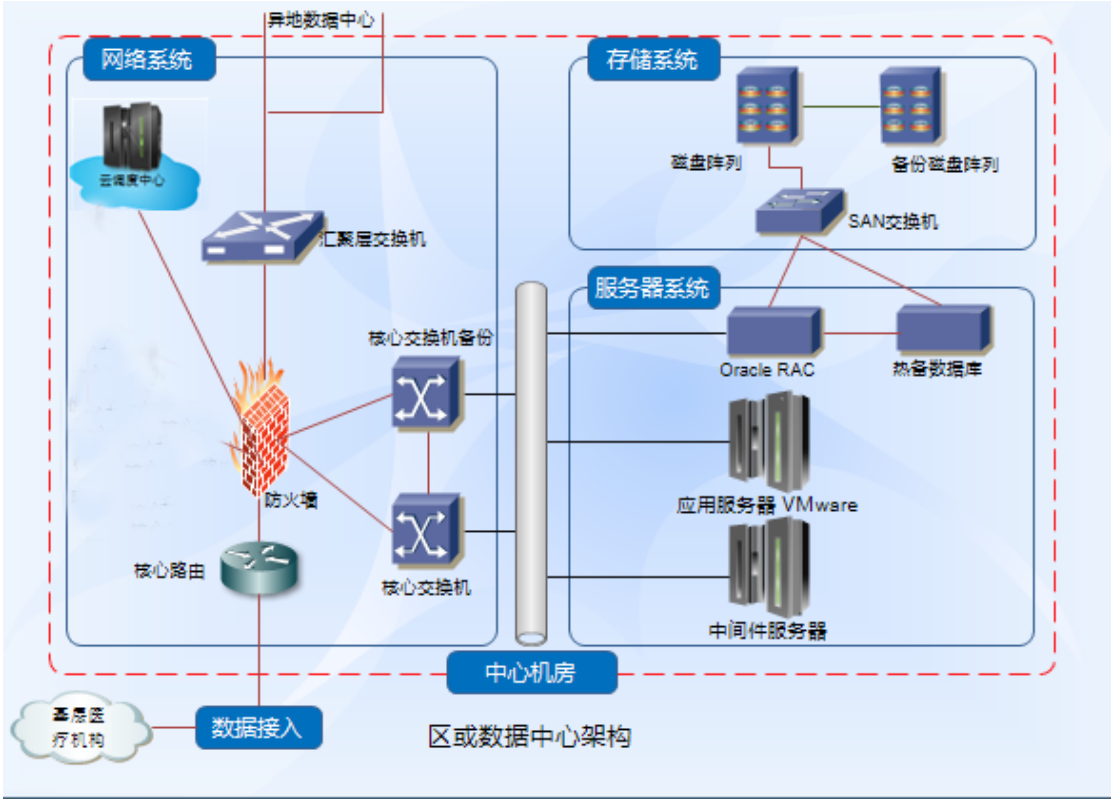
2.5 云数据安全管理

每天定时对系统与数据差异备份，每星期定时对系统与数据完整备份，为保证安全，备份数据异地存放。

3、 区域数据中心安全设计（如作为本区域中心则需考虑）

区域数据中心负责区域范围内的各医疗机构数据接入、存储与管理，是以医疗资源信息为主体，集计算机通信技术、分级诊疗数据和慢病患者日常行为数据管理为一体的专业化数据存储中心。

3.1 数据中心网络结构图



3.2 网闸/防火墙规则安全

区域数据中心架设在合作方指定的网络安全边界之内，对外网络边界采用防火墙+网闸，系统决定了哪些内部服务可以被外界访问；外界的哪些人可以访问

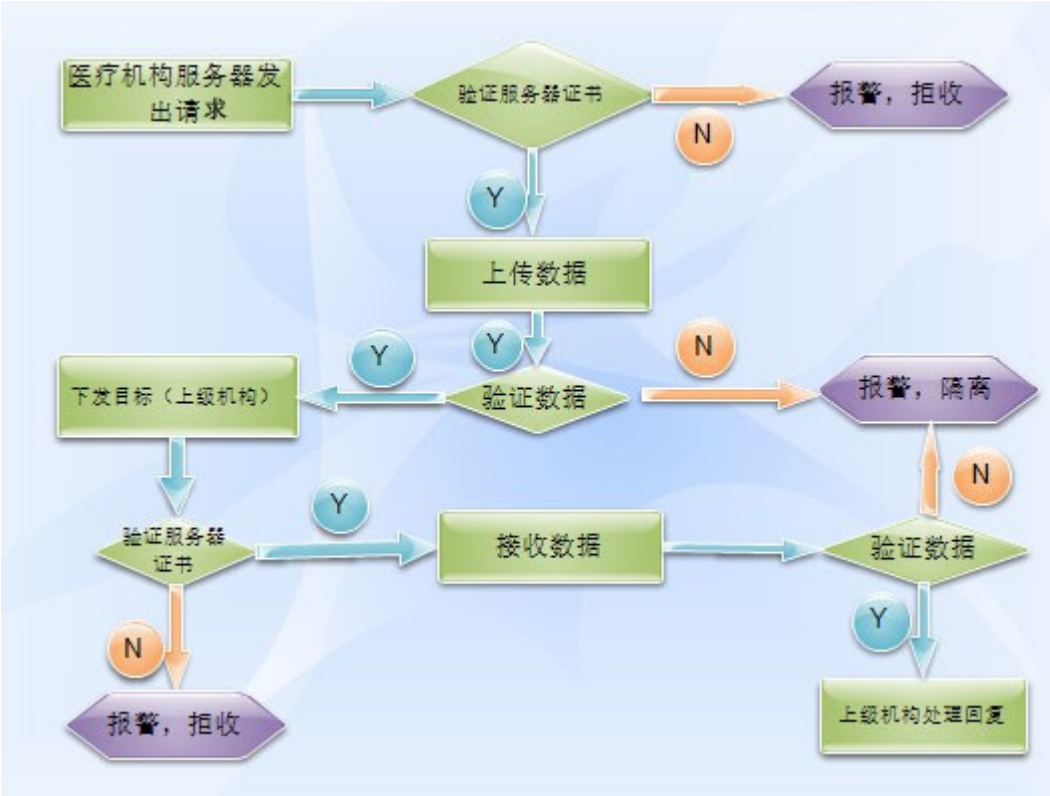
内部的哪些服务，及哪些外部服务可以被内部人员访问。所有来自和去往 Internet 的信息都必须经过防火墙，接受防火墙的检查。防火墙只允许授权的数据通过，并且防火墙本身也能够免于渗透。

- IP/MAC 地址的可信（类似于 DNA），生物身份。医疗机构前置服务器）
- 身份精细—MAC/用户的精确。（数据来源终端）
- 数据加密保护。
- 安全隔离。

3.3 通迅安全

- 通讯采用与受信设备签名认证+用户认证+密码认证+证书认证+数据加密传输（非对称加密），在授权的安全网络边界之内登录。确保用户数据不被监听、窜改、丢失、被盗等等，造成医生与患者隐私信息泄露。一旦数据异常服务器自动向管理员报警并隔离异常数据。
- 数据中心服务只被动接收授权医疗机构的授权医生主动发出的会诊医疗数据，而且这些数据只能在授权的安全网络边界之内经过层层认证后方能传输，确保用户数据不被监听、窜改、丢失、被盗等等，避免造成医生与患者隐私信息泄露。

3.4 数据传输安全：

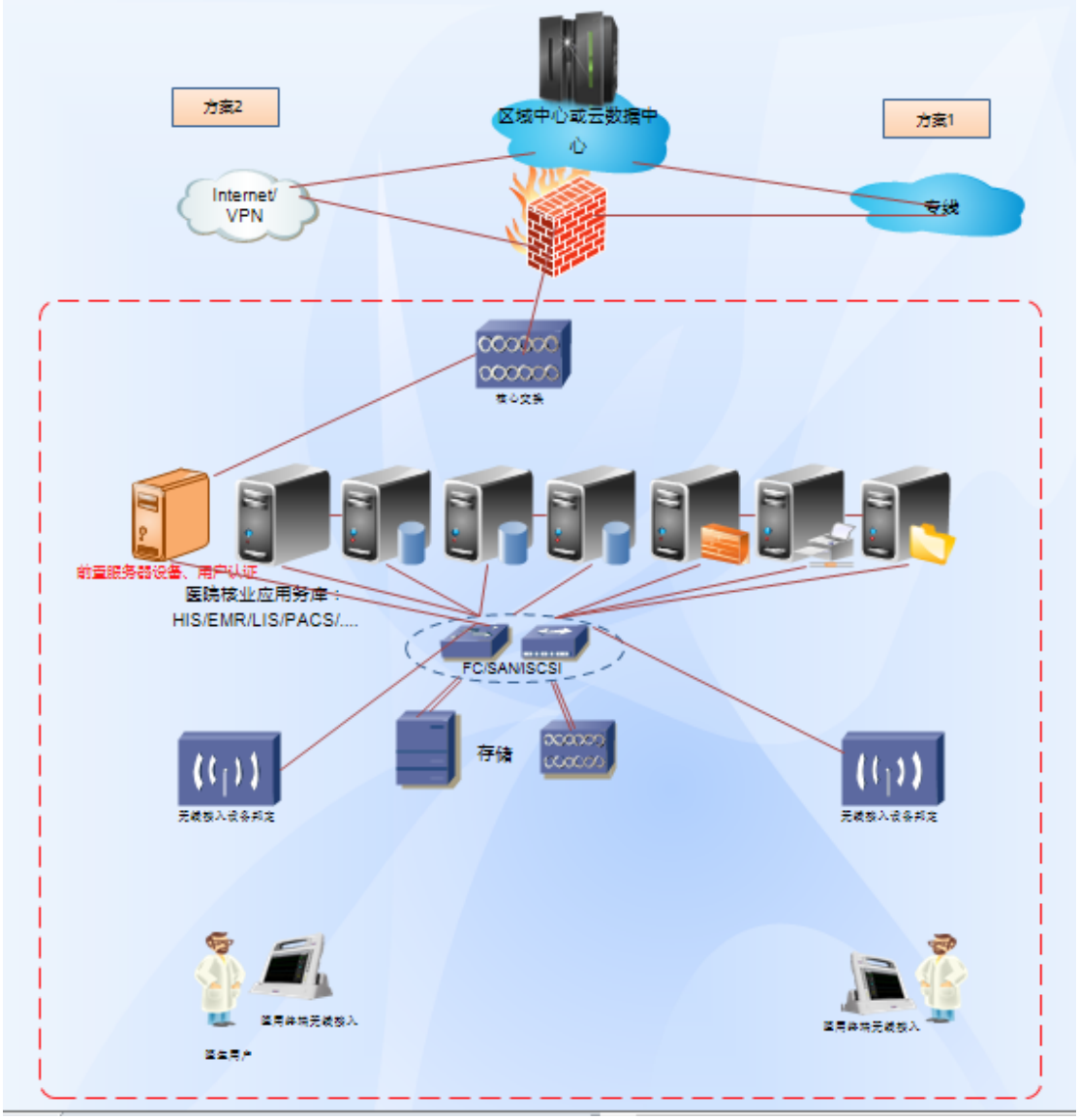


3.5 数据中心数据安全管理

每天定时对系统与数据差异备份，每星期定时对系统与数据完整备份，为保证安全，备份数据异地存放。

4、 院内系统接入安全部署

4.1 机构网络拓扑图



- 服务器存放于合作医疗机构的网络安全防护边界之内，同一局域网内通讯采用与受信设备签名认证+用户认证+密码认证+权限，禁止否认设备+用户权限之外所有服务，确保用户数据不被监听、窜改、丢失、被盗等等，避免造成医生与患者隐私信息泄露。
- 中心服务器只被动接收授权地区医院授权医生主动发出会诊医疗数据，而且这些数据只能在授权的安全网络边界之内经过层层认证后方能传输，确保用户数据不被监听、窜改、丢失、被盗等等，避免造成医生与