妇幼保健信息系统网络支撑平台技术指南

卫生部征求意见稿

中国疾病预防控制中心妇幼保健中心

中国卫生信息学会妇幼保健信息专业委员会

二００六年十二月

指导单位：卫生部信息化工作领导小组办公室

中国疾病预防控制中心

组织单位：中国疾病预防控制中心妇幼保健中心

中国卫生信息学会妇幼保健信息专业委员会

主要参与单位：苏州市卫生局

厦门市妇幼保健院

武汉市妇幼保健院

技术协作单位：杭州创业软件股份有限公司

厦门智业软件有限公司

武汉加州系统工程公司

主　编：张　彤、汤学军

副主编：（按姓氏汉语拼音排列）

陈小康、李　健、涂忆桥

主要编写人员：（按姓氏汉语拼音排列）

曹兴兵、何　俊、罗晓东、王　萍、吴建明、杨光彩、余小益、张人寿

目　录

1.引言

1.1 目的

按照卫生部《全国卫生信息化发展规划纲要〔2003-2010 年〕》精神，为了配合中国疾病预防控制中心妇幼保健中心关于《妇幼保健信息系统基本功能规范》和《妇幼保健信息系统基本数据集标准》等国家基础信息标准的制定与应用推广，满足各级妇幼保健机构开展妇幼卫生信息化建设的科学规划与设计的基本要求，实现妇幼保健信息网络系统建设的高效、实用、稳定、安全和互联互通，特制定《妇幼保健信息系统网络支撑平台技术指南》。

1.2 范围

本指南主要包括妇幼保健信息系统的开发与运行管理所需的网络支撑平台的总体结构、技术平台选择、系统集成、服务器与存储、数据库平台、信息安全体系等主要技术内容。本技术指南不包括妇幼保健信息系统运行所需客户端设备的有关技术要求内容。

本指南可供各级妇幼保健机构在进行妇幼保健信息网络系统建设的技术方案制定、工程招投标和建设实施过程中，结合《妇幼保健信息系统基本功能规范》和《妇幼保健信息系统基本数据集标准》等参考使用。

本指南的使用范围为各级妇幼保健机构和卫生行政部门、妇幼保健信息网络系统承建单位和工程监理单位等。

1.3 规范性引用文件

- 妇幼保健信息系统基本功能规范 (中国疾病预防控制中心妇幼保健中心)
- 妇幼保健信息系统基本数据集标准(中国疾病预防控制中心妇幼保健中心)
- GB/T 15237-1994 术语学基本词汇
- GB2887-89 计算机站场地技术条件
- GB9361-88 计算站场地安全要求

- GB50174－93　电子计算机房设计规范
- BMZZ1-2000 涉及国家秘密的计算机系统安全技术要求
- GB/T 18336-2001 信息技术 安全技术 信息技术安全性评估准则
- GB/T 8567-1988 计算机软件产品开发文件编制指南
- GB/T 11457-1995 软件工程术语

1.4 术语与定义

妇幼保健信息系统

指按照国家有关法律法规和政策、标准的要求，以计算机技术、网络通讯技术等现代化手段，对妇幼保健机构及相关医疗保健机构开展的妇幼保健服务工作各主要阶段所产生的业务、管理等数据进行采集、处理、存储、分析、传输及交换，从而为卫生行政部门、妇幼保健机构及社会公众提供全面的、自动化的管理及各种服务的信息系统。

妇幼保健信息系统网络支撑平台

支持妇幼保健信息系统开发、集成、运行和管理的软硬件基础平台，包括支持妇幼保健信息系统运行的网络基础设施平台，如服务器、存储、网络、操作系统、数据库等，以及支持妇幼保健信息系统开发及与其他异构信息系统集成的应用集成中间件平台。

应用集成中间件平台

应用集成中间件平台是指以业务为导向和驱动的、可快速构建和运行管理应用软件系统的基础软件平台，包括基础开发平台和应用集成平台两个部分。应用集成中间件平台主要能满足复杂应用软件系统构建和运行管理的如下要求：一是速度要求，通过基础开发平台提供的基本框架以及预置好的模块，能很快地开发出所需要的应用软件系统；二是灵活性要求，通过基础开发平台提供的开发与管理工具，能很方便地满足业务个性化的需求，以及在业务发展过程中变化的需求。三是集成性要求，通过应用集成平台为复杂应用软件系统提供了一个集成框架，不仅为集成同一平台上的各种不同软件提供了规则，还为集成其他应用软件和数据库系统提供了集成接口。

基础开发平台

基础开发平台为复杂应用软件系统的开发提供了一个基本框架，并有与之相应的、方便易用的开发与维护管理工具。这个框架给出了一些复杂应用软件的基本组成部分和实现方法，并且预置了很多供参考的软件模块。有了这样的准备，在基础开发平台之上开发管理软件就可以降低复杂性，省去很多基础性的研发工作，从而大大缩短研发周期，提高研发效率。

应用集成平台

应用集成平台为独立软件开发商、系统集成商和用户机构提供集成应用开发以及日常运营的平台，在此平台之上可有效整合各类业务应用系统，能支持异构系统之间的数据整合，快速实现应用程序节点部署以及各业务子系统之间的协同通讯，最终形成一个互联互通的业务协作网络，高效地管理、传递和展现整个业务过程中的相关信息。

数据接口

数据接口是指应用集成中间件平台软件模型定义的提供给各系统接入单位或应用系统开发商使用的统一 API，系统接入单位或应用系统开发商可通过该 API 进行系统接口实施工作，使各机构的应用信息系统可与上级数据中心进行实时或非实时的通讯，进行数据采集或数据交换等操作。数据接口根据各机构应用信息系统环境差异有不同技术体现，一般为各种环境下封装的组件或中间交换数据库定义。

1.5 缩写词

API	应用程序编程接口
B/S	浏览器/服务器体系结构
C/S	客户端/服务器体系结构
GIS	地理信息系统
HIS	医院信息系统
SOA	面向服务的架构
VPN	虚拟局域网络
XML	可扩展性标志语言

2.总体技术要求

妇幼保健机构承担着妇幼保健保健服务和相关妇幼卫生事务管理职能，由于其职能定位和所开展妇幼保健服务内容的特殊性和复杂性，妇幼保健机构开展各项常规业务活动所需使用和依赖的妇幼保健信息系统，具有信息管理的内容繁杂、管理周期长、覆盖人群广、涉及其他医疗保健机构和相关部门多等特点，其信息管理工作为属区域化、分级管理格局。同时妇幼保健信息系统及其网络支撑平台也是公共卫生信息大平台的有机组成。

2.1 设计原则

- 实用性

  使用方便，结构合理，经济实用，资源共享。

- 兼容性

  网络支撑平台的体系结构应与已有的业务系统兼容。

- 先进性

  采用最新软硬件技术，保持高起点。考虑系统未来功能升级的要求，使系统具有开放性、兼容性、扩展性。

- 标准化

  采用的各类数据接口标准、通讯协议、软硬件设施等应遵循国际、国内有关标准规范要求。

- 安全性

  建立严密的安全保障措施。充分应用身份识别与验证、访问权限控制等技术。

2.2 平台功能要求

- 为妇幼保健信息系统的开发、建立和运行管理提供标准化的基础应用构件和网络平台及数据库系统支撑。
- 能基于统一的数据传输与交换标准，实现不同通讯条件下的网络化的数据收集、存储、汇总和交换。
- 能基于统一的基本数据集标准，整合各类异构应用系统，实现各类历史数据

和相关业务数据的抽取、规范管理和共享利用。

- 为构建区域化的妇幼卫生决策支持平台提供中心数据库与联机分析系统支撑，提供综合查询、数据展示和信息发布服务。
- 具备信息标准与规范配置管理系统，对妇幼保健信息系统基本数据集标准、业务流程规范等进行便捷管理和版本控制。
- 具备网络安全保障体系，应包括防火墙系统、VPN 系统、病毒防护系统、备份与容灾，CA 认证系统、入侵侦测系统、加密/解密系统、网管系统等。

2.3 网络系统要求

- 区域化分级管理要求。根据妇幼保健信息管理与信息服务的需要，妇幼保健信息系统网络支撑平台必须实现横向连接辖区范围内各类开展妇幼保健技术服务的医疗保健机构，以及计划生育管理、户籍管理、民政、托幼机构等相关业务部门，纵向连接上、下级妇幼保健机构和卫生行政部门，实现区域化的网络互通和数据共享，并实现与公共卫生信息平台的互联互通。
- 继承与发展要求。由于妇幼保健信息系统的建设过程是一个随着相关业务发展而循序渐进、逐步扩展的过程，妇幼保健信息系统网络支撑平台必须在网络和软件模型方面，支持不同时期建立的应用系统、数据库系统和硬件设施之间能基于规范、统一的技术框架，互相兼容，实现继承与发展的和谐统一。
- 运维管理要求。妇幼保健信息系统网络支撑平台应支持集中监控、集中维护、集中管理的运维管理方式，实现面向系统和流程的管理。通过系统管理平台和流程管理平台的建设，解决网络管理、主机管理、应用管理、数据库管理等，并成立一套基于流程管理的维护体系，保证妇幼保健信息系统安全、稳定、高效的运行。

3. 平台总体框架

3.1 平台总体结构

妇幼保健信息系统是涉及众多相关医疗保健机构的业务管理信息系统，除了满足妇幼保健机构自身的各种业务需要以外，还需要与相关的外部业务系统以及其他有关妇幼卫生类业务系统进行整合集成，实现异构系统网络间的互联互通。妇幼保健信息系统网络支撑平台是支持妇幼保健信息系统开发、集成、运行和管理的软硬件基础平台，根据平台总体技术要求，其总体结构应包括两大基础平台：

一是支持妇幼保健信息系统开发及与其他异构信息系统集成的应用集成中间件平台。应用集成中间件平台是妇幼保健信息系统开发和应用集成的基础平台，是以业务为导向和驱动的、可快速构建和运行管理应用软件系统的基础软件平台，它主要提供妇幼保健信息系统建设的各种基础服务和基础业务组件，使整个妇幼保健信息系统的开发和运行更加方便快捷。同时还是一个消息交换中心，根据标准协议与规范向外部系统提供各种数据接口，实现与外部系统(如医院信息系统、社区卫生服务信息系统、疾控信息系统、公安户籍管理系统等)的集成。

二是支持妇幼保健信息系统运行的网络基础设施平台。网络基础设施平台主要包括服务器、存储、网络、操作系统和数据库系统以及计算机房和信息安全体系等，它是支撑整个妇幼保健信息系统安全、稳定、正常运行的基础保障系统。

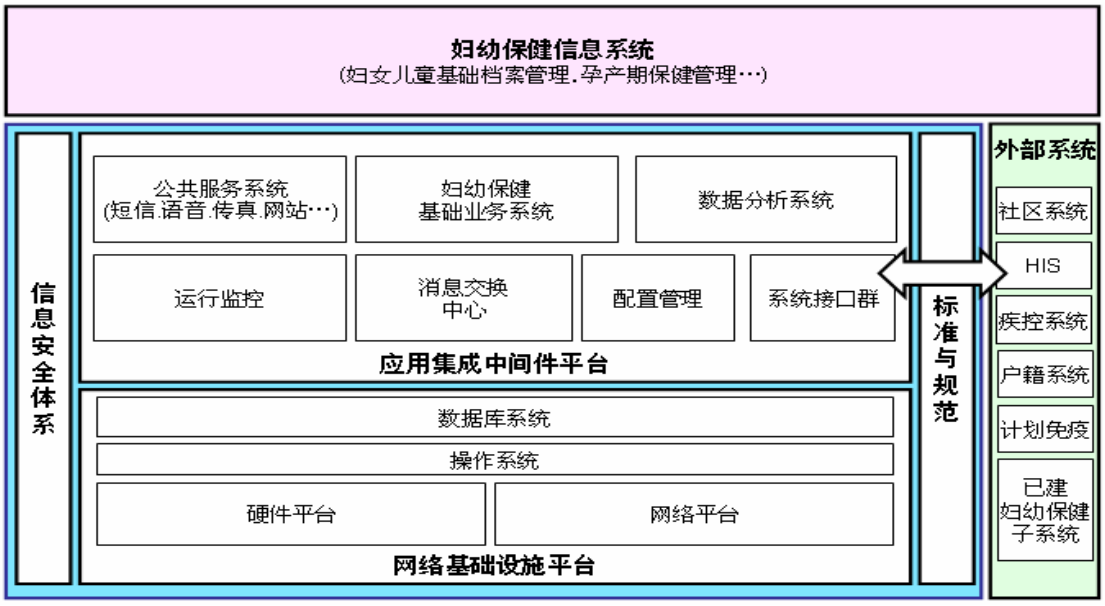

图 1 妇幼保健信息系统网络支撑平台总体框架

3.2 平台建设与运行管理模式

妇幼保健信息系统网络支撑平台的建设和运行管理，原则上以市级为妇幼保健信息区域化管理的基本建设和运行管理单位，区县级是利用市级妇幼保健信息系统及网络支撑平台负责妇幼保健信息收集、上报和服务的基本信息管理单位。

市级妇幼保健信息系统网络支撑平台，通过公用网络通信平台，横向连接辖区范围内各级各类开展妇幼保健技术服务的医疗保健机构，以及计划生育管理、户籍管理、民政、托幼机构等相关业务部门，纵向连接上、下级妇幼保健机构和卫生行政部门，实现区域化的网络互通和数据共享，并实现与本市公共卫生信息平台的互联互通。

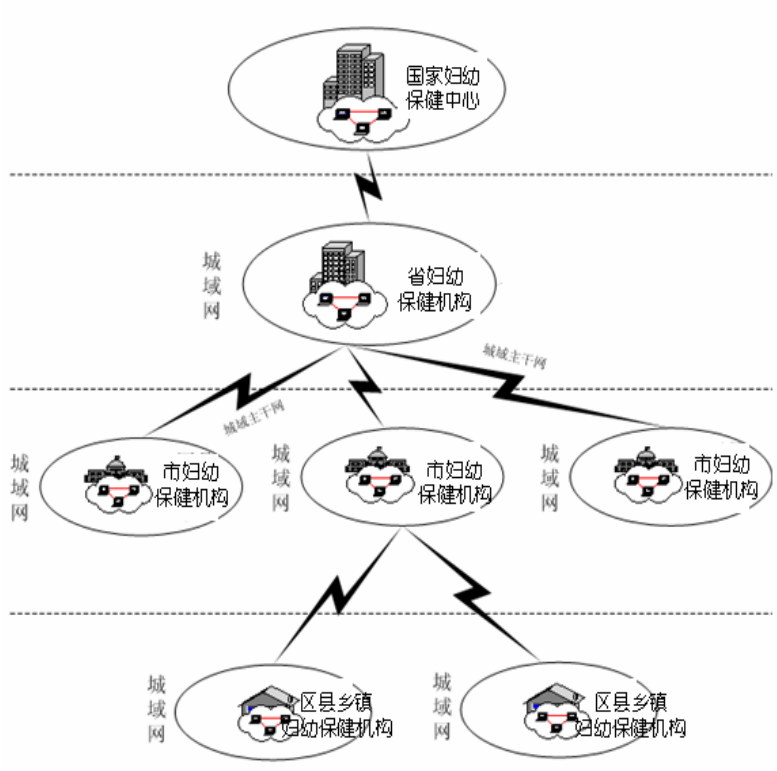

图 2 妇幼保健信息系统网络支撑平台运行管理模式

3.3 平台数据管理模式

妇幼保健信息系统网络支撑平台的数据管理模式可分为两种，即：数据集中模式和数据交换模式。数据集中模式是指整个应用系统采用 B/S 架构，各基层妇幼保健业务机构采用网络直报方式进行业务操作和信息共享，妇幼保健业务数据全部保存在市级妇幼保健数据中心，而各基层妇幼保健业务机构不保存相关的业务数据。

数据交换模式是指在各基层妇幼保健业务机构独立安装使用的应用系统基础之上，依据各种数据接口标准通过集成平台实现对分布式数据的收集、汇总和共享，各基层妇幼保健业务机构的应用系统中都保存有自己的数据，市级妇幼保健数据中心只是存放了用于数据汇总分析和数据交换共享的数据。

各地妇幼保健信息系统网络支撑平台的建设可根据本地实际条件，选择采用数据集中模式或数据交换模式，也可采用两种模式相结合的方式。

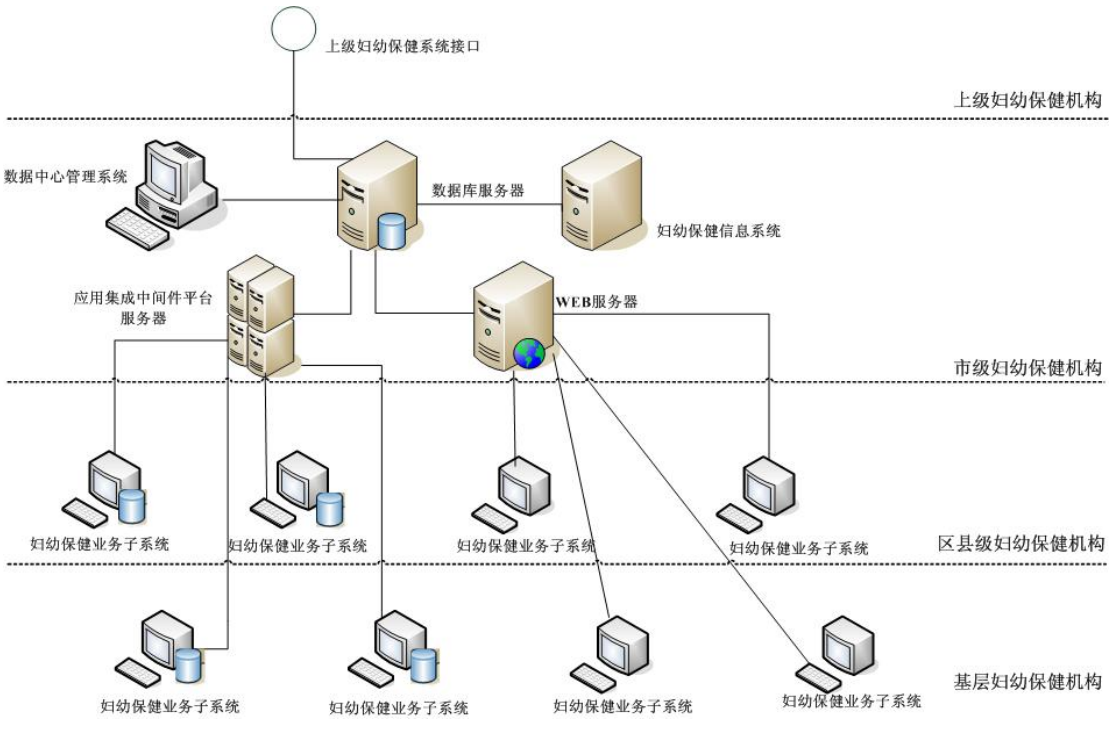

图 3 妇幼保健信息系统网络支撑平台数据管理模式

4. 应用集成中间件平台

应用集成中间件平台主要能满足复杂应用软件系统构建和运行管理的如下要求：一是速度要求，通过基础开发平台提供的基本框架以及预置好的模块，能很快地开发出所需要的应用软件系统；二是灵活性要求，通过基础开发平台提供的开发与管理工具，能很方便地满足业务个性化的需求，以及在业务发展过程中变化的需求。三是集成性要求，通过应用集成平台为复杂应用软件系统提供了一个集成框架，不仅为集成同一平台上的各种不同软件提供了规则，还为集成其他应用软件和数据库系统提供了集成接口。应用集成中间件平台主要包括基础开发平台和应用集成平台两个部分。

基础开发平台为复杂应用软件系统的开发提供了一个基本框架，并有与之相应的、方便易用的开发与维护管理工具。这个框架给出了一些复杂应用软件的基本组成部分和实现方法，并且预置了很多供参考的软件模块。有了这样的准备，在基础开发平台之上开发管理软件就可以降低复杂性，省去很多基础性的研发工作，从而大大缩短研发周期，提高研发效率。

应用集成平台为独立软件开发商、系统集成商和用户机构提供集成应用开发以及日常运营的平台，在此平台之上可有效整合各类业务应用系统，能支持异构系统之间的数据整合，快速实现应用程序节点部署以及各业务子系统之间的协同通讯，最终形成一个互联互通的业务协作网络，高效地管理、传递和展现整个业务过程中的相关信息。

4.1 技术体系

应用集成中间件平台应采用消息机制，基于消息中间件的方式进行交互，符合.NET 或 J2EE 等成熟的技术框架， 并符合 XML 技术数据传输格式规范。根据不同基础条件，妇幼保健信息系统可选择 C/S 或 B/S 设计模式，而妇幼保健数据中心的各种数据查询、联机分析系统应主要采用 B/S 设计架构。

4.2 消息交换中心

应用集成中间件平台的消息交换中心应基于 SOA 架构的交换总线，它主要是完成各种异构系统间消息的传输、转换、过滤与路由等，通过服务总线（Service Bus）和服务或流管理器来连接服务和提供服务请求的路径。流管理器处理定义好的执行序列或服务流将按照适当的顺序调用所需的服务来产生最后的结果。在消息交换服务总线(Message Bus)上再增加服务注册中心(Portal)，以及系统运行监控系统（Monitor），与业务系统连接的适配器，就构成了以消息为基础，以面向服务为导向的妇幼保健信息系统网络平台接口模型，从而实现对妇幼保健信息系统与其他异构系统的集成。

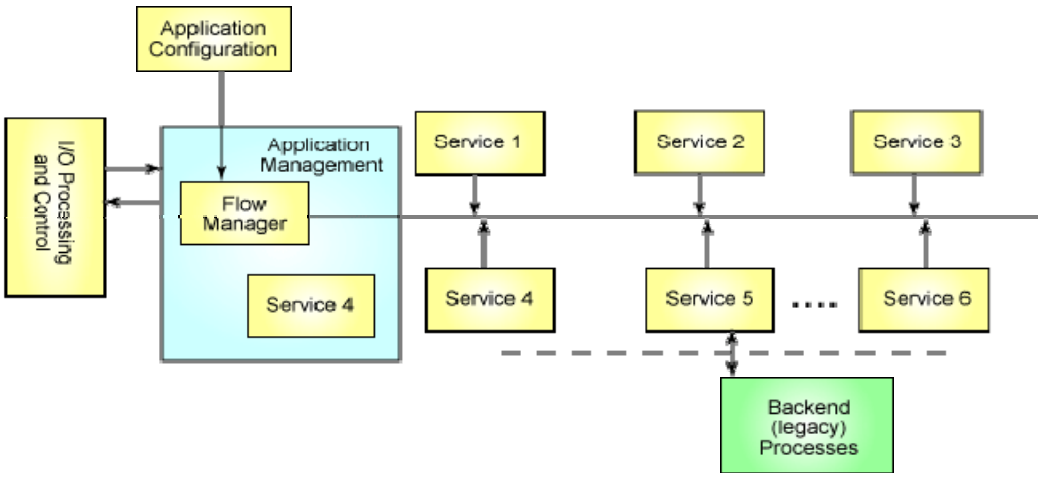

图 4 基于 SOA 架构的消息交换中心

4.3 配置管理

应用集成中间件平台应具备配置管理功能，包括配置和管理各网络接入机构接入适配器的参数，运行配置文件分发，各业务信息系统提供的功能服务注册中心，发布/订阅主题管理，消息流转，接入接点与接入接点之间数据交互权限与安全认证管理，各种标准和协议的管理。

4.4 运行监控

应用集成中间件平台应具备运行监控功能，包括对各接入点业务消息流转进行监控，管理和远程控制各接入点机构通讯前置机应用，监控接入点机构通讯前置机上源适配器和目标适配器运行状态，各接入点运行日志远程查看，统计和查询流转消息，监控接入点应用、中心负载情况。

4.5 公共服务系统

应用集成中间件平台应提供短信、语音、传真、邮件、网站、数据管理、系统框架、GIS 等基础公共服务组件供妇幼保健信息系统使用，以提高妇幼保健信息系统的开发效率。

4.6 基础业务系统

应用集成中间件平台应根据《妇幼保健信息系统基本功能规范》和《妇幼保健信息系统基本数据集标准》提供妇幼保健信息系统所需要的各种共性的基础业务组件，以提高妇幼保健信息系统的开发效率和整个系统的规范性。如：数据采集表自定义系统、用户角色权限管理系统等。

4.7 数据分析系统

应用集成中间件平台应包含数据分析系统以实现对区域化妇幼保健中心数据库进行综合查询和数据分析；数据分析系统应以《妇幼保健信息系统基本数据集标准》为基础，采用数据仓库技术和 GIS 技术进行数据分析和数据展示。

4.8 系统标准接口群

应用集成中间件平台应遵循妇幼保健信息系统集成标准协议，向各种业务系统提供标准的数据接口，以实现妇幼保健信息系统与其他各系统间的数据交换与共享。

数据接口技术可以选用以下几种方式：

序号	分类	作用与备注
1	标准接口方式	发送单个请求和接受响应，主要用于实时的业务请求，通常嵌入原系统进行工作。可用于实时远程调用最新的个案信息等业务场景。
2	批量数据采集接口方式	两点之间发送批量数据，主要用于定时数据传送方式，用于批量数据上传到数据中心或从数据中心下载各类名册信息等业务场景。
3	服务接口方式	用于向别的应用系统实时提供数据，接受别的系统发送的数据请求，返回本地业务数据，通常用于各类遗产系统或已建系统的接口改造工作。
4	文件接口方式	用于各类文件型数据的导入和导出工作，应支持常规的EXCEL，DBF，TXT 等格式。 通常用于各类遗产系统的数据导入导出，以及报盘系统制作。
5	发布订阅接口方式	订阅某个主题的数据，当有其他系统向该主题发送数据时可自动开始接收数据，用于一对多的广播式数据分发。通常用于各种监测业务，当监测指标发生变化时及时通知其他系统。

4.9 异构系统集成规范

序号	系统分类	异构系统集成处理方式建议
1	不准备继续投入使用的遗产系统	通过应用集成中间件平台从遗产系统中最大限度地导出和存储历史数据
2	继续投入使用的已建系统	通过应用集成中间件平台的接口方式实时或定时同步数据与数据集成
3	已开始建设的业务系统	通过应用集成中间件平台提供的基础业务组件和接口数据规范进行集成与改造
4	未建系统	通过应用集成中间件平台提供的基础业务组件和数据接口规范统一开发

5. 网络基础设施平台

5.1 网络拓扑结构

网络基础设施平台由内、外两大网络部分组成。外部网络对外收集和提供信息(向下级部门采集与提供信息，向上级数据中心报送信息)，内部网进行信息管理和系统开发，两网之间用防火墙分隔。外部对内部网络的访问则需要通过地址映射，身份查询等一系列安全检查机制才能进行，访问策略的制定是灵活的，可根据具体情况随机配置。内部网络再分子网，依据功能、性质划分，子网间的访问也是受控的。外部网络的安全性主要依靠“虚拟专用网”的功能和路由器上的访问控制表来保障。

对于实时多媒体应用本着中央控制的原则对有条件的用户开放，运维管理中心应具备监视和控制的手段，避免网络拥塞和信息流的非必要的重复性传输。整个平台应采用先进的网络管理和网络安全措施与策略，网络管理及安全策略应从系统管理的角度出发，实现网络、应用系统、数据库与主机系统以及安全防护措施和策略的一体化管理，选择适当的防火墙和数据加密技术。

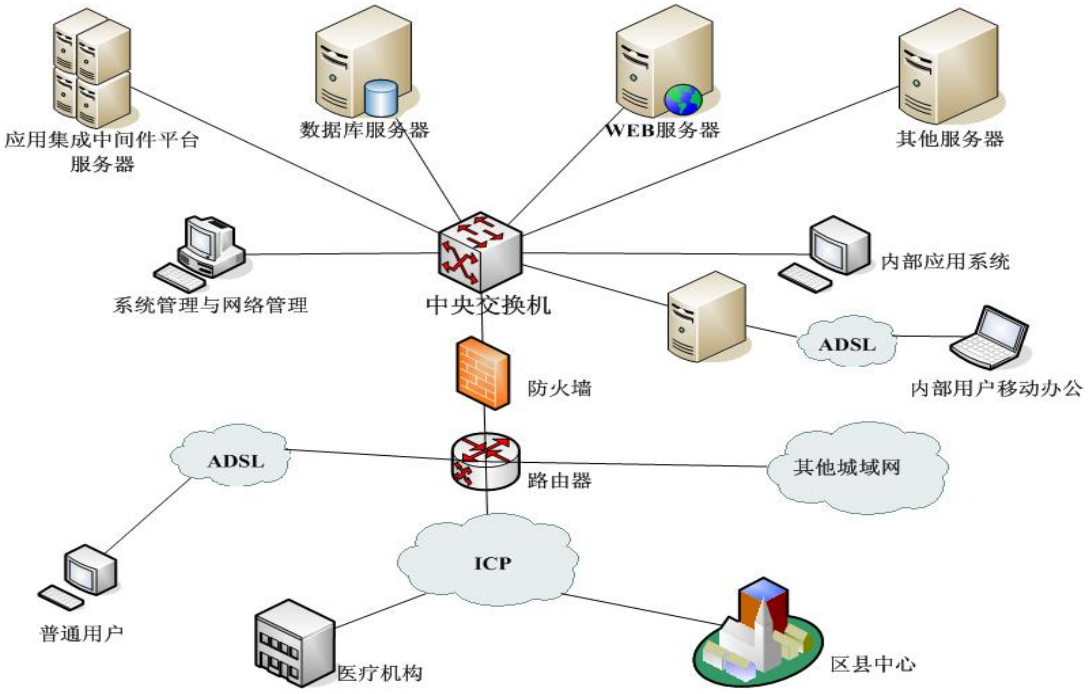

图 5 网络基础设施平台拓扑结构

5.2 硬件系统

网络基础设施平台的硬件系统一般包括：数据库服务器、备份服务器、应用服务器等；交换机、路由器、防火墙、VPN 等网络设备；存储设备如磁盘阵列、磁带库等。

网络基础设施平台的硬件系统配置，应根据当地实际业务需求、网络覆盖范围和规模以及经济条件，本着经济、实用、高效合分步实施的原则，选择适当的建设方案。

本指南按初级、中级、高级分别列出网络基础设施平台硬件系统配置的三种建议方案。

5.2.1 初级配置方案:

初级配置方案包括建立一个较规范的、安全的市级网络基础设施平台所必需的各项基本设备设施，包括：数据库服务器、应用服务器；交换机、路由器、防火墙、VPN 设备；磁盘阵列等。

性能要求:

- **服务器:**
  - 高性能 PC 服务器，各服务器均独立配置
  - 要求 1～2 个处理器、4GB 以上内存
- **磁盘阵列:**
  - 磁盘阵列系统 1 套
  - 按区域数据估算存储容量
  - 支持分区、快照、克隆等基本功能
  - 支持在线扩容，无须停机
- **交换机、路由器:**
  - 企业级路由式核心交换机
- **防火墙、VPN 设备:**
  - 企业级硬件防火墙，具备 VPN 功能
- **网络防病毒系统:**
  - 针对运行 Windows 系统的服务器、数据库系统进行网络防病毒监控

- 对连接到专网的各接入点前置服务器的网络病毒防范
- 要求采用中央集中控制和管理

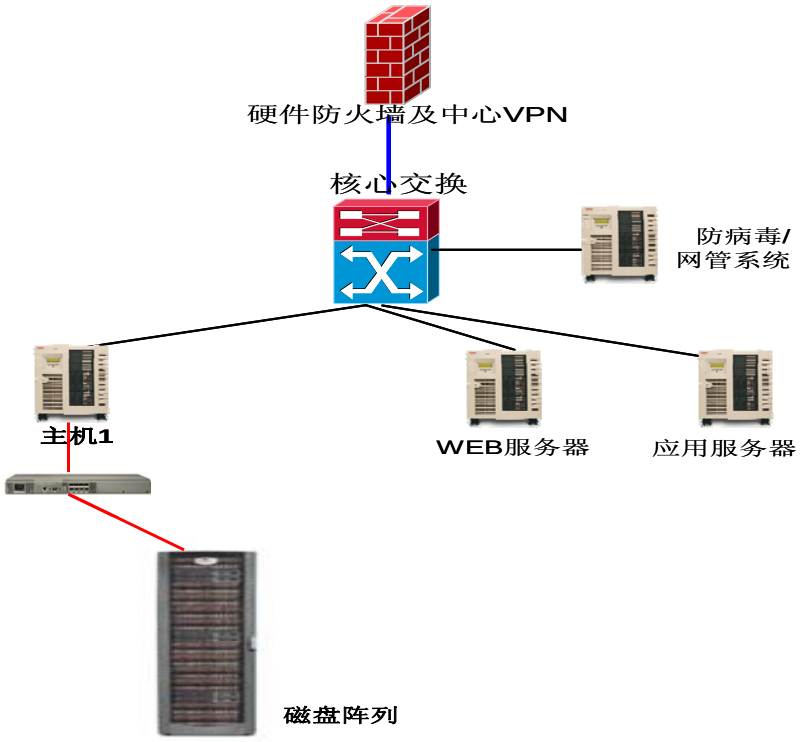

图 6 网络基础设施平台硬件系统初级配置方案

5.2.2 中级配置方案:

中级配置方案是在初级配置方案基础上,通过增加关键服务器系统的双机热备或集群模式,强化了服务器系统的运行稳定性和可靠性。并增加了离线备份系统,加强数据安全保障。此外还提升了磁盘阵列、VPN 设备等系统性能指标。

性能要求:

- **服务器:**
  - 高性能 PC 服务器,各服务器均独立配置
  - 要求 1~2 个处理器、4GB 以上内存
  - 集群模式
- **磁盘阵列:**
  - 全或半光纤磁盘阵列系统 1 套
  - 按区域数据估算存储容量

- 支持分区、快照、克隆等基本功能
- 支持在线扩容，无须停机

- **网络备份系统:**
  - 磁带库 1 套
  - 网络备份软件 1 套
  - 独立的备份服务器
- **交换机、路由器:**
  - 企业级路由式核心交换机
- **防火墙、VPN 设备:**
  - 企业级硬件防火墙
  - 独立的硬件 VPN 设备
- **网络防病毒系统:**
  - 针对运行 Windows 系统的服务器、数据库系统进行网络防病毒监控
  - 对连接到专网的各接入点前置服务器的网络病毒防范
  - 要求采用中央集中控制和管理

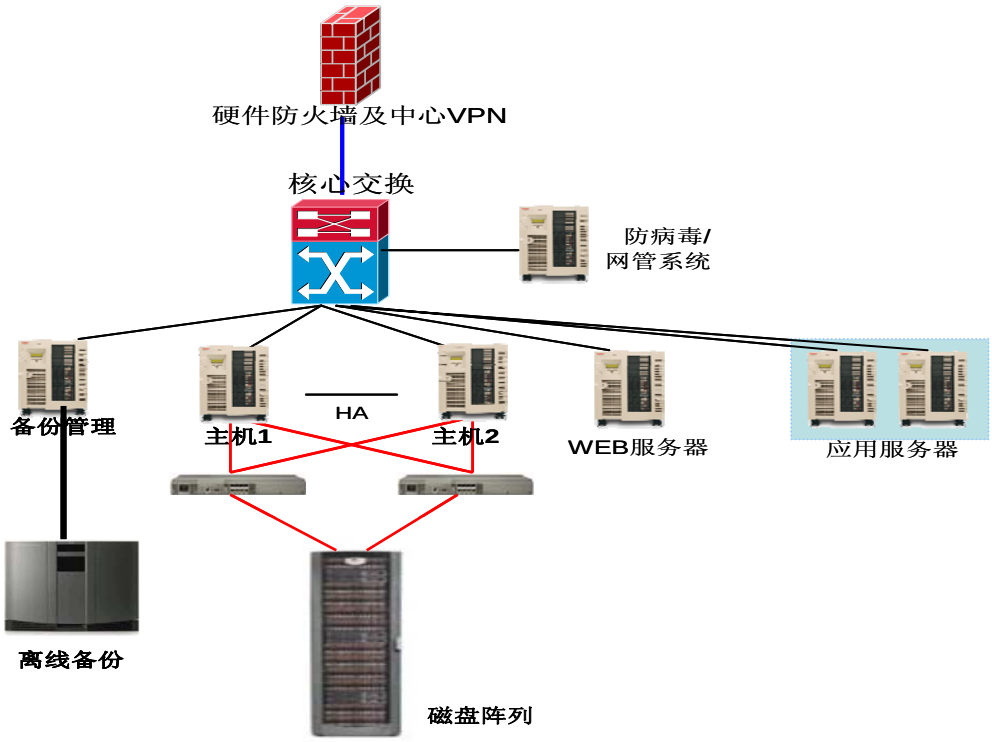

图 7 网络基础设施平台硬件系统中级配置方案

5.2.3 高级配置方案:

高级配置方案是在中级配置方案基础上，将数据库服务器主机由 PC 服务器更换为小型机系统，进一步增强了数据库系统的运行稳定性和负载能力。并将主要的网络设备改造为双机负载均衡模式，极大地提高了网络交换性能和网络安全保障能力。

性能要求:

- **服务器:**
  - UNIX 小型机，各服务器均独立配置
  - 要求 1～2 个处理器、4GB 以上内存
  - 集群模式
- **磁盘阵列:**
  - 全或半光纤磁盘阵列系统 1 套
  - 按区域数据估算存储容量
  - 支持分区、快照、克隆等基本功能
  - 支持在线扩容，无须停机
- **网络备份系统:**
  - 磁带库 1 套
  - 网络备份软件 1 套
  - 独立的备份服务器
- **交换机、路由器:**
  - 企业级路由式核心交换机
  - 双机负载均衡模式
- **防火墙、VPN 设备:**
  - 企业级硬件防火墙
  - 独立的硬件 VPN 设备
  - 双机负载均衡模式
- **网络防病毒系统:**
  - 针对运行 Windows 系统的服务器、数据库系统进行网络防病毒监控
  - 对连接到专网的各接入点前置服务器的网络病毒防范

❒ 要求采用中央集中控制和管理

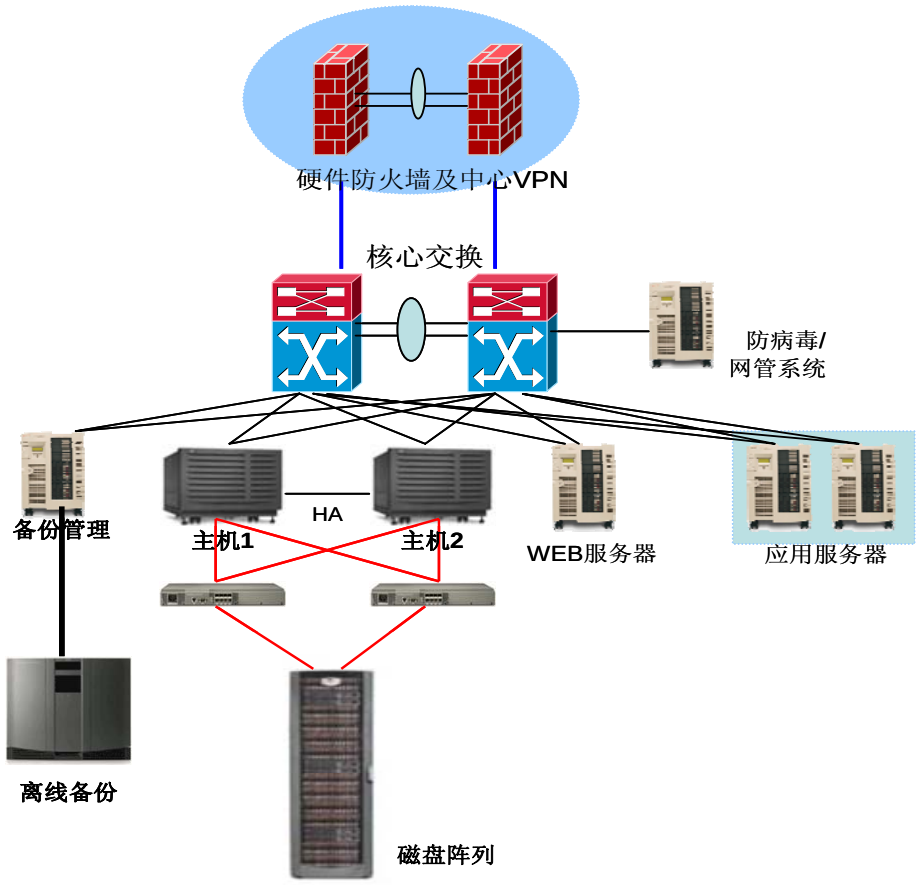

图 8 网络基础设施平台硬件系统高级配置方案

5.3 组网方式

建设妇幼保健信息系统网络平台时，应首先考虑采用 VPN 技术来建设逻辑业务网。利用 VPN 网的主干交换机完成底层安全措施，既可防止其他业务系统用户未经授权进入和使用妇幼保健信息网络平台的信息资源，也可防止本系统用户进入其他的业务逻辑网络。本指南分别列出目前通用、成熟的三种组网建议方案。

5.3.1 专线组网方案

主要是指分组交换网、DDN、FR、ATM 等专线连接方案。分组交换网的速率较低、租用费较高；DDN 速率较高、租用费高；帧中继（FR）速率较高、租用费较低；ATM 速率较高、费用最高。除费用和速率方面外，还需考虑接入的可靠性。

性能要求:

- 应主要依托卫生行业现有主干网络平台（如公共卫生网、医保网等），组建妇幼 VPN 专网;
- 妇幼保健信息网络数据中心网络接入带宽：10M 或以上;
- 各接入点的网络带宽：2M 或以上;
- 移动接点或单机接点可采用拨号方式通过 Internet 建立与妇幼保健信息网的 VPN 连接。

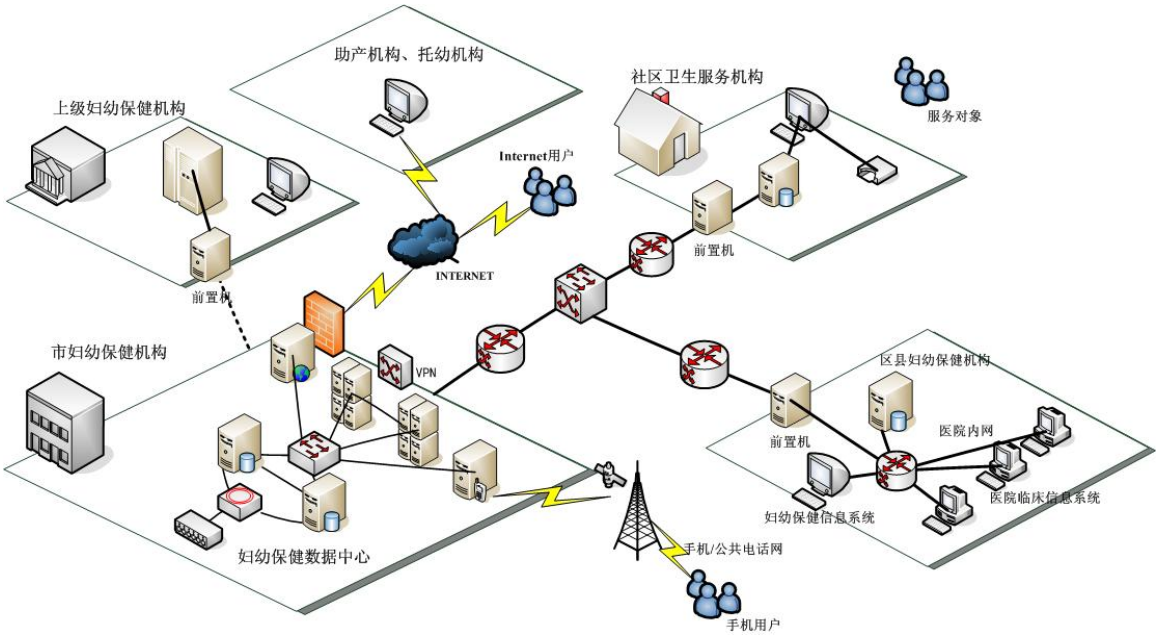

图 9 基于 VPN 的专线组网方案示意图

5.3.2 公网宽带组网方案

全国各大城市已经建立了一个结构完整、技术先进、门类齐全、适度超前的基础通信网络体系。互联网宽带的普及，使能接入公网的各业务机构可方便地利用宽带连接与数据中心建立 VPN 网络。

性能要求:

- 公网宽带网络;
- 通过 ADSL 等宽带方式接入 Internet,在公网上建立与妇幼保健信息网的 VPN 连接;
- 妇幼保健信息网络数据中心网络接入带宽：1M 或以上;

- 各接入点的网络带宽：512K 或以上；
- 移动接点或单机接点可采用拨号方式通过 Internet 建立与妇幼保健信息网的 VPN 连接。

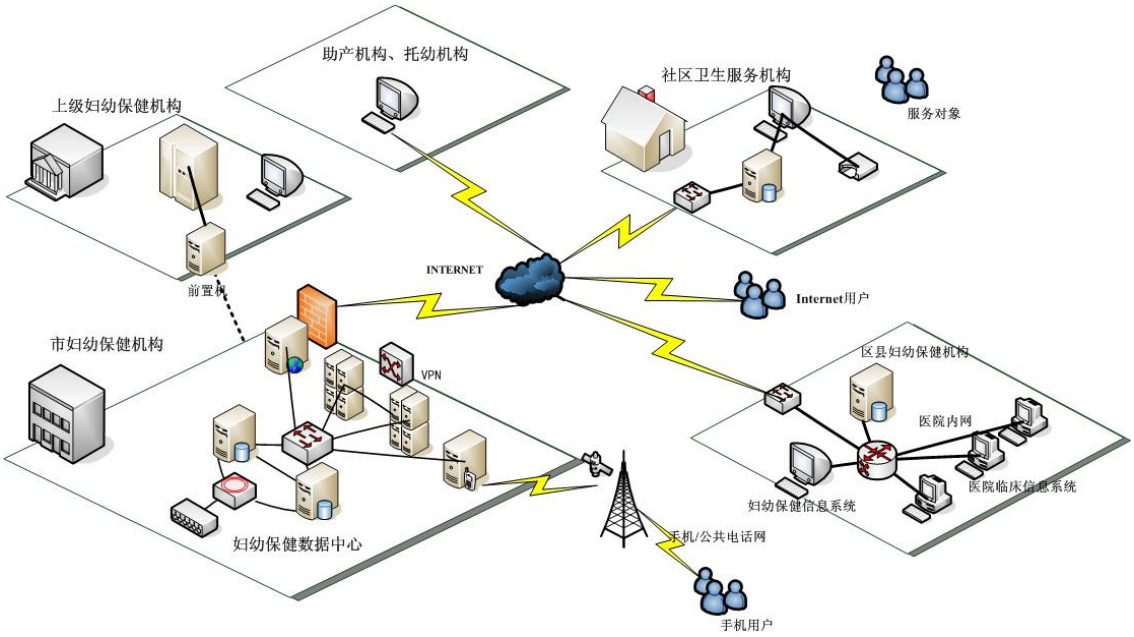

图 10 基于 VPN 的宽带组网方案示意图

5.3.3 电话拨号组网方案

拨号连接的方式主要有两种：一种是 PSTN，即公用电话网；另一种是 N-ISDN，即窄带综合业务数字网。前者的速率低，使用的是模拟语音信道，覆盖面广，费用低；后者的速率居中，使用的是数字信道，覆盖面居中，费用中等。

性能要求：

- 公用电话网或窄带综合业务数字网；
- 各接入点通过电话线拨入到妇幼保健数据中心的 Modem 池，建立数据链路；
- 妇幼保健信息网络数据中心网络接入带宽：128K 或以上；
- 和各接入点的网络接入带宽：56K 或以上；
- 移动接点或单机接点可采用拨号方式通过 Internet 建立与妇幼保健信息网的 VPN 连接。

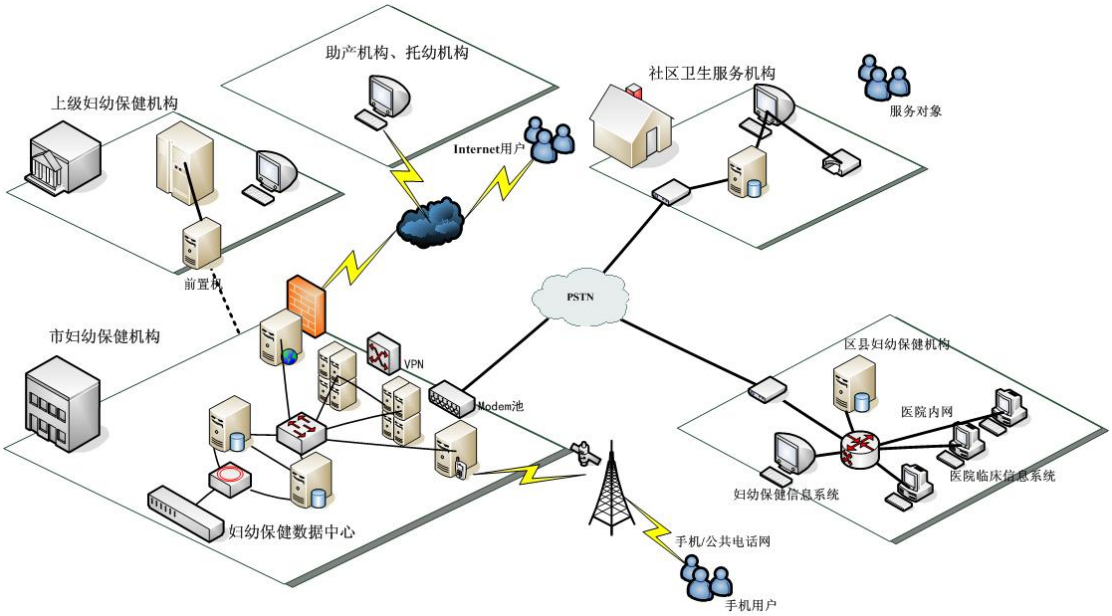

图 10 基于 VPN 的电话拨号组网方案示意图

5.3.4 各种组网方案的优缺点分析

序号	比较项目	专线	公网宽带	电话拨号
1	带宽	2M 或 10M	512K 或 1M	56K 或 128K
2	稳定性	高	中	底
3	实施难度	视当地运营商网络覆盖度	易	易
4	实施成本	高	中	低
5	适合场景	大数据量、高用户规模，长期在线，适合批量定时数据和实时数据交换	操作频率低的业务，一般需要时才拨号建立网络	少量数据传输的业务，需要时才拨号建立网络，无法长期在线和实时数据交换

5.4 机房环境

妇幼保健信息系统网络中心机房应满足国家标准(GB50174－93)电子计算机房设计规范的要求，达到如下标准:

- 标准机房建设;
- 精密空调系统;
- 为所有服务器提供在线式 UPS 供电系统; 建议采用双路供电;
- 标准的机房安全准入和保障系统。

5.5 操作系统

操作系统的选择依主机的选择而不同，采用小型机可选用 Unix 或 Linux; 采用 PC 服务器一般可选用 Windows 操作系统。

5.6 数据库系统

妇幼保健信息系统网络支撑平台建议选用大型通用关系型数据库系统，优先选择支持 XML 和 GIS 的关系型数据库平台。数据库系统选型必须满足安全可靠、可扩展、跨平台、易操作; 同时应采用分布式的原则，避免负载沉重和单点故障问题，如有条件可选择做双机热备或双机负载均衡。

妇幼保健信息系统数据库的表结构设计必须遵循《妇幼保健信息系统基本数据集标准》。

6 信息安全体系

妇幼保健信息网络平台是由计算机及其相关的设备、设施(含网络)构成的，并按照一定的应用目标和规则对各种信息进行采集、加工、存储、传输、检索等处理的人机系统。因此，它潜在的威胁可能来自于各类人员（包括系统内、外人员），人员对系统的攻击动机各异、形式多样，可能出现在可以访问妇幼保健信息网络平台的任何地方,表现为有意或无意的破坏行为。也可能来自于各种灾害、设备和设施的故障，灾害或设备的威胁主要表现为物理安全威胁。

妇幼保健信息系统网络支撑平台的建设必须遵循国际、国内标准和规范，建立信息安全体系,通过系统的技术防护措施和非技术防护措施来保障整个妇幼保健信息系统的安全。信息安全体系包括基础设备安全、软件安全、数据安全和非技术防护措施等。

6.1 基础设施安全

- 妇幼保健信息系统网络支撑平台应具备性能完善的网络安全基础设备。包括网络防火墙、入侵检测、病毒防范、用户识别等信息安全软硬件系统，并设专人进行日常监督管理与更新;
- 各类服务器均应放置在具有防火墙保护的独立网段中，以确保服务器安全;
- 关键设备应有冗余后备系统;
- 具有足够容量的 UPS 后备电源；电源要有良好的接地。

6.2 软件安全

- 系统软件和应用软件应具有访问控制功能，包括用户登录访问控制、角色权限控制、目录级安全控制、文件属性安全控制等;
- 系统软件(包括操作系统，数据库等)和应用软件等应定期进行完全备份，系统软件配置修改和应用软件的修改应及时备份，并做好相应的记录文档;
- 及时了解系统软件和应用软件厂家公布的软件漏洞并进行更新修正;
- 应用软件的开发应有完整的技术文档，源代码应有详尽的注释;
- 使用基于 PKI-CA 体系的数字证书实现各业务应用系统的用户身份验证、数

字签名等功能。

6.3 数据安全

- 数据库应设置预定的备份策略进行本地备份，有条件的可做异地备份;
- 严格按照用户级别来授权用户对数据和资料的访问;
- 关键数据的修改记录应记录详细的操作日志，以备追查;
- 数据的传输与关键敏感的数据的存放需进行一定的加密处理。

6.4 非技术防护措施

- 信息基础设备应安置在专用的机房，具有良好的电磁兼容工作环境，包括防磁、防尘、防水、防火、防静电保护，抑制和防止电磁泄漏;
- 对机房出入进行有效控制，对重要服务器系统和中心机房进行电视监控，确保设备安全;
- 对涉密网的环境因素实施监控和警卫，预防人为威胁;
- 集中建设网络支撑平台监控中心，进行统一安全监控;
- 建立健全相关网络安全管理责任制度。