附件1

浙江省卫生业务网非公立机构接入规范（试行）

第一章 概述

## 1.1目标

根据《基本医疗卫生与健康促进法》《网络安全法》《密码法》《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》《网络安全审查办法》以及网络安全等级保护制度等有关法律法规标准，为指导非公立机构规范、有序、安全的接入卫生业务网，加强网络安全管理，防范网络安全事件发生，特制定本接入规范。

## 1.2背景

近年来，随着我省医疗卫生体系建设的持续深化与加速发展，非公立医疗机构对接入省级卫生业务专网的需求显著增强。为应对医疗服务规模扩张、提升行业服务质效、强化信息安全和资源共享能力，现基于现有卫生业务专网实施系统性升级，通过延伸网络覆盖范围、融合新一代信息技术，着力破解传统医疗数据孤岛难题。此次升级以构建标准化、开放性、互联互通的综合网络平台为核心路径，推动实现全省卫生业务专网统一架构规划与运维管理，促进公立与非公立机构间资源动态调配及业务协同，同步构建涵盖数据加密、权限管控的多层次安全防护体系，确保医疗信息全流程可追溯、可监管。最终通过数字化平台赋能，加速区域医疗健康服务体系转型升级，为构建高效整合型医疗卫生服务体系奠定智能化基石。

## 1.3基本原则

**分级管理。**各级卫生健康行政部门负责管理本级卫生业务网的迭代升级、准入审核、安全监管等工作。按照医疗机构属地管理的原则，实现卫生业务网分级管理，非公立机构的网络接入点原则上应与医疗机构许可证的发放地相一致。

**统一标准。**省卫生健康信息中心制定全省卫生业务网非公立机构接入规范，推动全省非公立机构接入卫生业务网，实现“愿接尽接”。

**加强安全。**各级卫生业务网主管单位要充分考虑网络安全和数据安全，发挥主体责任，加强安全监管。

第二章 重点建设内容

## 2.1迭代升级卫生业务网

按业务发展需要，在现有的卫生业务网基础上，拓宽医疗机构接入的范围，各级卫生健康行政单位按照技术兼容性、安全保障、数据共享与隐私保护、法规遵循与监管以及服务质量等要求，负责本级卫生业务网迭代升级工作，指导非公立机构规范、有序、安全接入卫生业务网。

### 2.1.1总体架构

全省卫生业务网在纵向上由三个主要层级构成：省级骨干网、市级骨干网、县级骨干网，确保了信息在各级卫生健康行政单位及各级卫生业务网之间的顺畅流通和高效管理。

根据业务需求，省市县三级卫生健康行政单位要在现有的卫生业务网架构上完成迭代升级，增加非公立机构网络域。非公立机构网络域优先接入同级健康云网络接入区，通过健康云与公立机构网络域互通，也可直接接入同级卫健部门骨干节点。属地为县级的非公立机构直接接入县级卫健部门骨干节点。非公立机构可通过专线或互联网IPSec方式接入。

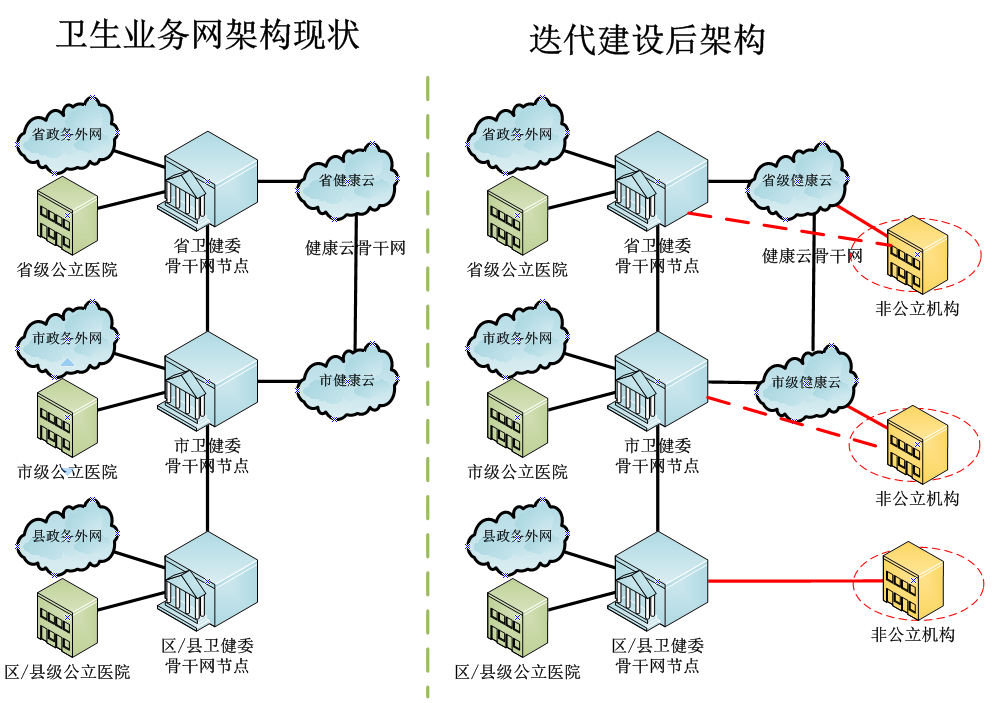


图1 浙江省卫生业务网总体架构示意图

### 2.1.2职责划分及要求

（1）省级市级卫生业务网管理单位职责

省级市级卫生业务网管理单位负责本级卫生业务网的业务指导和运行监管。

（2）县级卫生业务网管理单位职责

县级卫生业务网管理单位负责本级卫生业务网的业务指导和运行监管，按照本规范要求，承担本级非公立机构的接入工作和安全管理职责。

（3）健康云网络接入区归属单位职责

按照本规范要求，承担本级非公立机构的接入工作和安全管理职责。

（4）相关运营商职责

按照本规范要求，承担各级非公立接入区和接入机构的专线或互联网线路建设、运维、安全管理等职责，配合各级卫生业务网管理单位工作。

（5）接入机构职责

接入机构定期做好运行维护工作，确保接入线路稳定运行，遵守相关政策和法规，落实安全防护和数据保护措施，制定网络安全相关制度，快速响应和处理安全事件，融入本级网络安全工作体系。

### 2.1.3建设非公立机构接入区

非公立机构接入区用于本级非公立机构接入和网络域的边界管理。针对不同的接入方式，接入区应部署路由器、IPSec设备等网络设备和防火墙等安全设备，实现具有访问控制、入侵检测（防御）、病毒防护等能力，提升专网网络安全、威胁防护能力。非公立机构接入区如下图所示：

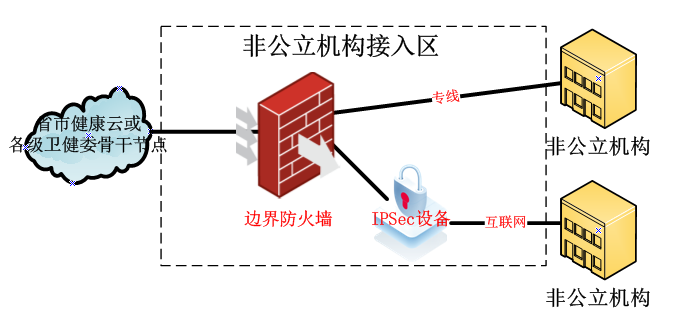


图2 非公立机构接入区示意图

各级非公立机构接入区归属单位，可利旧或新建本级网络安全资源池，为接入机构提供安全服务，形成规范的安全防护体系标准，实现安全事件感知、阻断、处理的全流程化，提升卫生业务网安全水平。

表1 接入区安全能力清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 部署位置 | 设备类型 | 必（可）选 | 功能简述 |
| 1 | 接入区 | IPSec设备 | 二选一 | 通过互联网线路，利用IPSec技术实现逻辑网络与物理网络分离，具备统一管理、访问控制、入侵防御、病毒防护等能力。 |
| 2 | 接入区 | 路由器 | 通过专线，实现非公立机构接入。 |
| 3 | 接入区 | 下一代防火墙 | 必选 | 含基本网络防火墙功能、访问控制功能、攻击防护、Web防护、用户认证功能、链路负载均衡功能、流量控制、资产识别、IPSec VPN等功能。 |
| 4 | 网络安全资源池 | 日志审计 | 必选 | 通过对各类日志的全面采集、解析和全局关联分析，全面感知各种安全威胁和异常行为事件。提供事前可预警、事后可审计的安全管理能力，满足网络安全法、等级保护2.0、数据安全法等相关法律法规对日志数据的留存及审计要求。 |
| 5 | 数据库审计 | 必选 | 实时对数据库的访问行为进行审计监控、风险评估与综合分析。通过对用户访问数据库行为的记录和分析，帮助全面感知、定位风险；同时通过统计数据库性能情况，为数据库性能调优提供方向。满足各类法令法规（如等保2.0、分级保护、企业内控、SOX等）对数据库安全的要求。 |
| 6 | 运维审计 | 必选 | 含基本堡垒机功能，用户认证，资产管理，策略管理，工单管理，运维管理，任务管理等功能 |
| 7 | 态势感知 | 必选 | 对各种WEB攻击、邮件社工类攻击进行检测；多维度全方位发现失陷主机；识别内网中横向扩散及渗透攻击行为；对检测对象的会话特征进行多维度监控统计；对流量中的资产进行统计分析；提供综合威胁分析、主机威胁分析、外部威胁分析等多个智能报表；提供综合管理和关联分析能力。 |
| 8 | 漏扫扫描 | 必选 | 集主机安全扫描、网站安全扫描、数据库安全扫描、弱口令发现和基线配置核查于一身，帮助用户提高网络安全防护性能和抗破坏能力的产品 |
| 9 | 终端准入 | 可选 | 以旁路准入控制技术为基础，对终端行为、访问信息特征进行监控，建立综合的网络和终端技术防护体系，基于多种技术建立“事前控制、事中监控、事后审计”全生命周期安全机制，提供终端网络接入控制功能，防止非授权终端接入内网，对接入终端的安全性进行检查。若对接区未涉及终端可不做要求。 |
| 10 | 终端杀毒 | 可选 | 对主机进行安全加固，防止恶意代码入侵。 |

## 2.2接入机构要求

### 2.2.1资质要求

非公立机构在申请接入卫生业务网前，需提交相关资质证明（如医疗机构执业许可证、与信息安全文件等），由各本级卫生业务网主管部门对资质进行审核。

### 2.2.2网络要求

（1）专线方式：与公立机构网络域逻辑或物理隔离，不得与互联网连接；互联网IPSec方式：逻辑网络与物理网络分离，逻辑网络不得与互联网连接。

（2）链路测试指标：吞吐量(Throughput)100%，丢包率(Frame Loss)<0.1%。

（3）带宽要求：专线链路带宽不少于10Mbps，带宽可按需扩容；IPSec加密通道带宽不少于10Mbps。

### 2.2.3安全要求

接入机构须按照《网络安全法》《信息系统安全保护条例》等法律法规，落实信息系统等保定级和相应网络数据安全防护，尤其对存储有大量公民个人敏感信息的信息系统，须至少按照等保二级以上的标准构建安全防护体系。

#### 表2 接入机构安全能力清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 部署位置 | 设备类型 | 必（可）选 | 功能简述 |
| 1 | 接入机构 | 交换机或路由器 | 二选一 | 通过专线，实现非公立机构接入。 |
| 2 | 接入机构 | IPSec终端设备 | 通过互联网线路，利用IPSec技术实现逻辑网络与物理网络分离，具备统一管理、访问控制、入侵防御、病毒防护等能力。 |