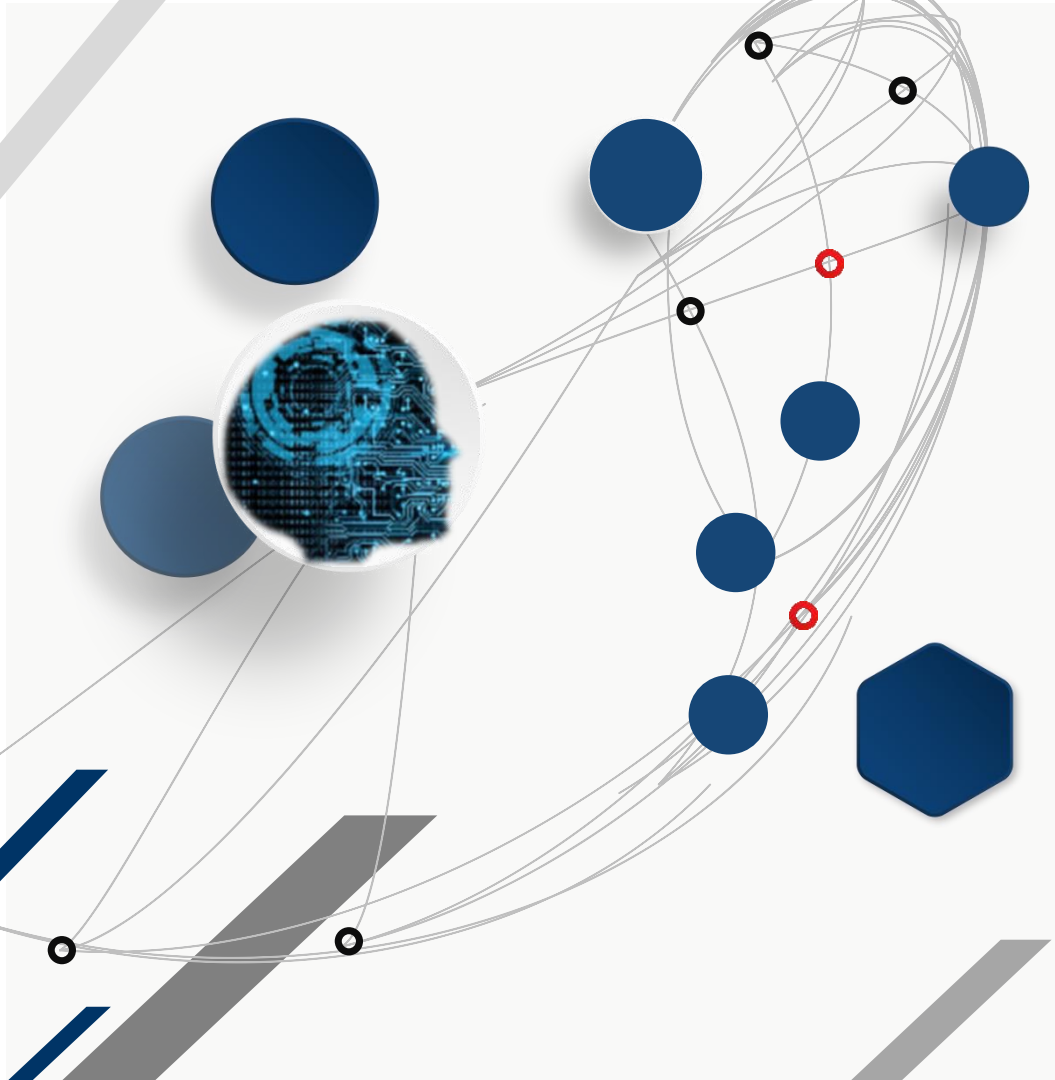


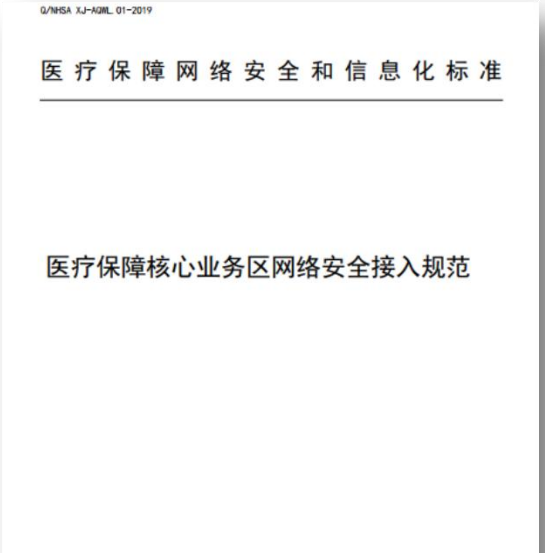
医保定点机构接入医保骨干网络政策解读

目录

医保网络接入相关的政策

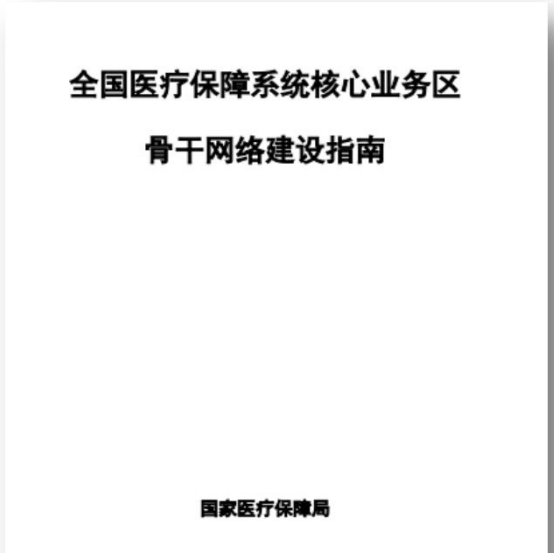
发布机构：国家医疗保障局网络安全与信息化领导小组办公室

2019年7月



为接入医保网提出基本要求

2019年12月



接入医保网的安全性建设较为详细的建议

医保网接入规范的适用范围

核心业务区横向接入

1. 三级医院、二级医院
2. 社区诊疗机构、村医诊所
3. 城乡各类定点药店

人社、卫健、民政、公安、税务等部门网络对接

接入方式解读

《医疗保障核心业务区网络安全接入规范》列示的接入方式

专线

专线是指在广域或城域连接中使用光纤，或者租用运营商SDH/MSTP、 DWDM链路、 PTN等进行互联的。xDSL等其他接入方式不属于专线

定点机构需支付更高月租，适配中大型医院与药店

政务外网

指国家电子政务外网和各级党政部门已建成的非涉密网。

外网仅覆盖横向接入的政府部门

VPDN网络

VPDN虚拟专用拨号网是运营商基于L2TP等技术为客户提供的一种相对可控的网络接入方式。这种接入方式可以提供对终端的认证功能，数据经过隧道传输。

费用适中，线路覆盖广，有手机信号的地方都能覆盖

核心业务区网络接入安全规范解读-终端安全

点对网模式：

接入终端要符合医疗保障部门的安全规范，并采取以下措施：

（1）接入终端应专机专用，不得连接互联网及其它网络，严禁处理涉密信息。

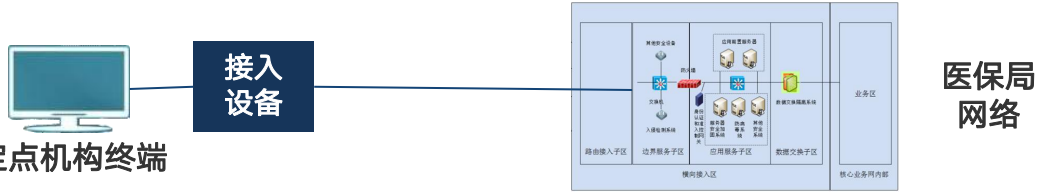
（2）接入终端应通过客户端安全监控和管理软件、符合国密算法的加密等技术手段进行安全管理，

（3）接入终端应安装杀毒软件，并确保病毒库及时更新，防范恶意代码。

（4）应使用医疗保障部门颁发的医疗保障数字证书进行用户身份认证。

（5）加强移动存储介质管理，严控数据输入输出，防止数据泄漏

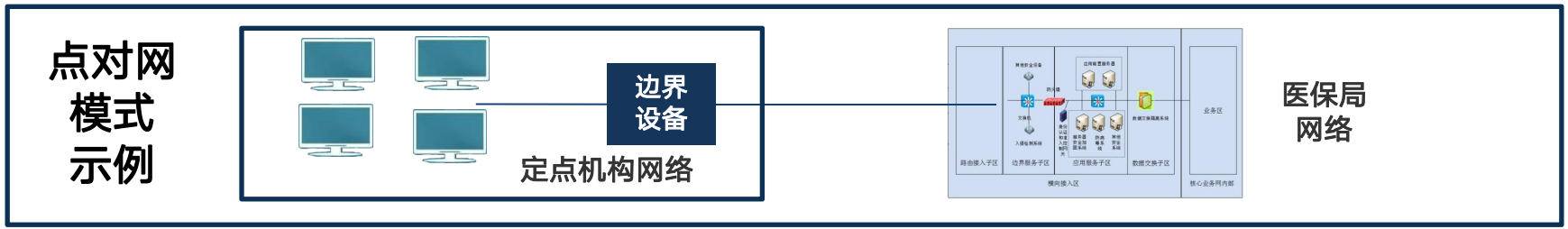
点对网模式示例



核心业务区网络接入安全规范解读-终端安全

网对网模式：

1. 接入单位网络须符合等保三级要求
2. 接入医疗保障核心业务区网络应采取访问控制、数据加密、身份认证等安全防护措施。
3. 在访问医疗保障业务应用时，须使用医疗保障部门颁发的数字证书进行用户身份认证



目录

《医保网络核心业务区骨干网络建设指南》的进一步指引

7　定点医药机构横向接入要求

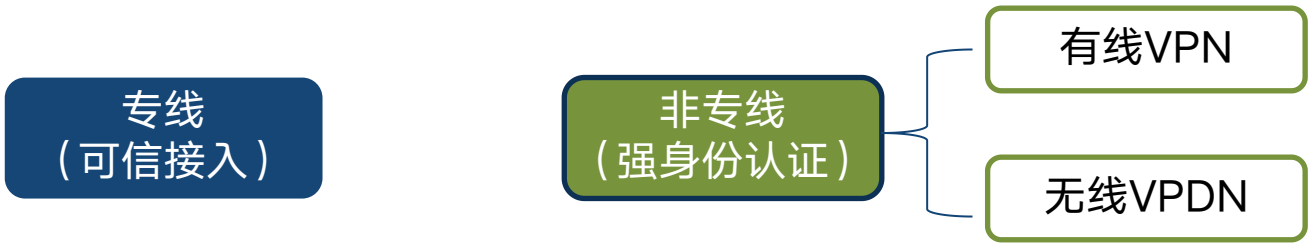
定点医药机构横向接入分为两种情况：

通过运营商专线形式接入方式，此种接入方式在链路层认定为可信接入，仅做在网络边界进行防护（部署防火墙），不进行准入认证。

通过非专线方式接入，须通过使用隧道加密技术和医保核心业务区 CA 强身份认证方式进行准入，同时接入设备须在同级医保局安全接入管理平台进行统一认证纳管后，才能允许访问医保核心业务区网络，非专线接入方式分为无线 VPDN 接入方式和有线 VPN 方式接入。

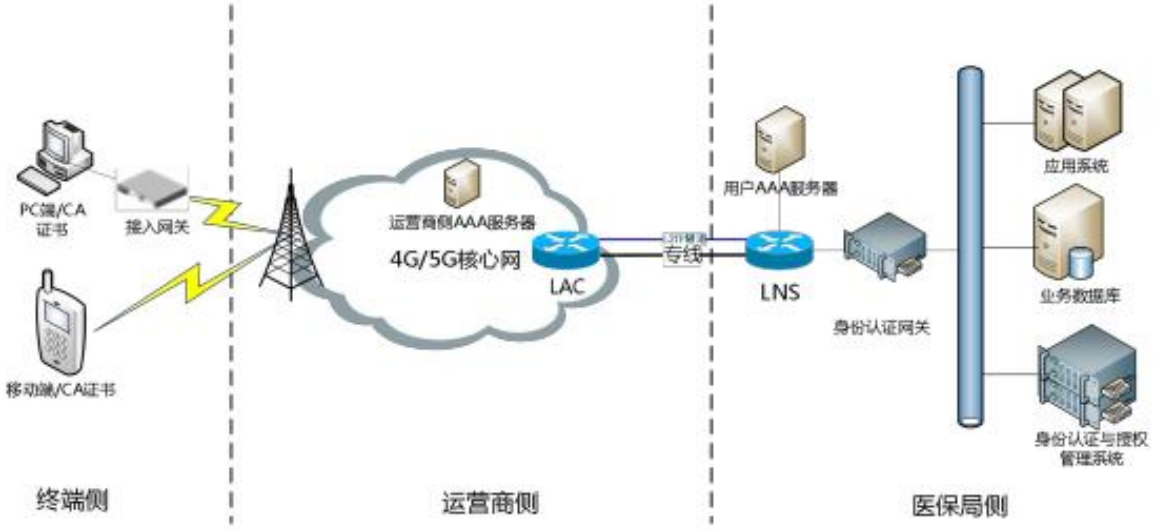
7.1　网络接入方式

定点医药机构（定点医疗机构和定点零售药店）主要通过专线、有线 VPN、无线 VPDN 方式接入医保核心业务区。



《医保网络核心业务区骨干网络建设指南》对接入方式的示范

7.1.2.2.1 无线 VPDN 方式



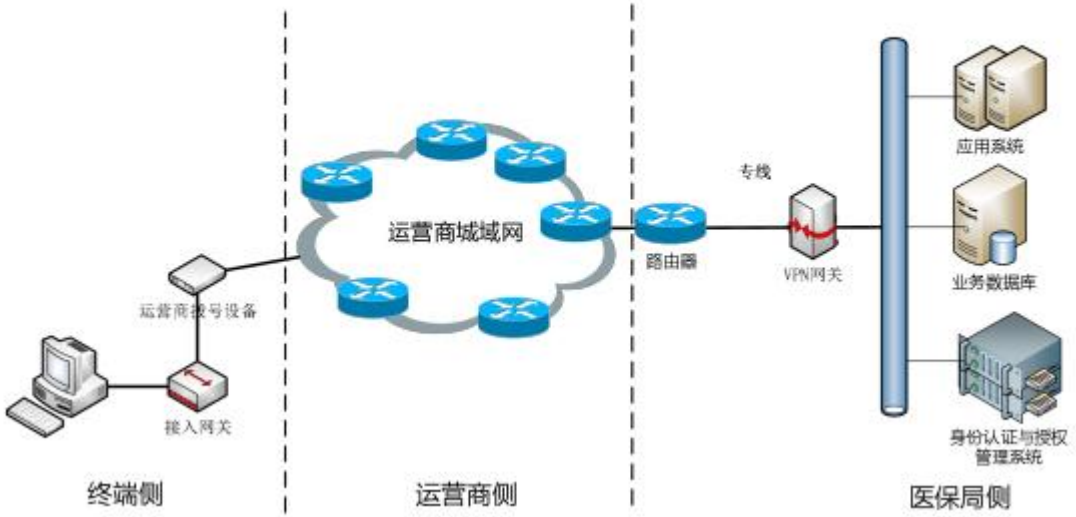
特点分析：

1. 与有线方式相比，线路覆盖更广、应用场景更多
2. 用户侧部署不穿墙、不拉线，部署较为便捷

1. 在定点机构部署带有国密密码模块、VPDN 功能的接入网关
2. 医保局侧路由器（LNS）通过专线方式和运营商侧路由器互联，与运营商 LAC 建立 L2TP 隧道。
3. 运营商侧具备第一次AAA认证，省医保局具备第二次AAA 认证完成鉴权、地址分配等功能。
4. VPDN 网络组成包括 4G 号卡、接入终端（具备国密模块）、LAC、LNS、AAA 服务器、专线实现 VPDN 接入，为定点医药机构接入医保核心业务区提供通道。

《医保网络核心业务区骨干网络建设指南》的进一步指引

7.1.2.2.2 有线 VPN 方式



特点分析：

1. 多数机构已布设线路，可以利旧；
2. 原有线路需按医保要求进行配置改造

1. 定点医药机构可以利用不具备互联网功能的专线与医保局建立 VPN 隧道（如 IPSec VPN）完成地方医保业务网的接入建设。
2. 在定点机构部署具有国密密码模块和 VPN 功能的有线接入网关；医保局部署 VPN网关。
3. 有线接入网关上连运营商提供的拨号设备，下连定点机构 PC 终端。通过 IPsecVPN 技术完成专用隧道建立、地址分配等功能，隧道建立后通过医保局端 CA 进行认证和准入。
4. 采用该方式要求所有接入点不能访问互联网，可以通过 VPN 终端和运营商网络策略设置实现。

《医保网络核心业务区骨干网络建设指南》对证书的要求

7.2 安全接入部署要求

国家局 CA 系统作为整个医保局身份认证系统的信任源头，是医保身份认证系统的最高权威，实现总体政策、管理制度和运作规范的制定和审批。地方医保局通过本级区域内部署的证书综合管理系统或证书综合管理系统（区县版）进行数字证书的生命周期管理（包括证书申请、证书更新、证书注销、证书冻结、证书解冻、证书查询等），由国家局 CA 系统统一签发数字证书，实现证书分散申请、集中生产。

解读：

1、证书必须由国家局CA系统统一签发（根证书在国家局）

2、各地使用的身份认证系统都要使用统一的数字证书

汇报完毕 谢谢聆听

运筹帷幄 赋能政务信息化

汇报人：锐捷网络公司