重庆市沙坪坝区医疗保障局文件

沙医保发〔2024〕14号

重庆市沙坪坝区医疗保障局

关于规范定点医药机构接入医保信息平台

专网的通知

各定点医药机构：

为进一步规范定点医药机构网络接入方式，防范重大数据和网络安全风险，根据《重庆市医疗保障局网络安全和信息化领导小组办公室关于规范定点医药机构接入医保信息平台专网的通知》（渝医保网信办〔2023〕1号）要求，结合沙坪坝区实际，沙坪坝区医保局对定点医药机构和云HIS接入重庆市医保信息平台核心业务区网络（以下简称“医保专网”）进行规范。现将有关事项通知如下：

一、网络接入规范

（一）组网模式。各定点医药机构的网络接入模式为“网对网”和“点对网”。其中“点对网”模式是指接入单位只将单个或多个终端连接到医保专网。“网对网”模式是指接入单位将其单位内部网络按照一定的安全保障措施连接到医保专网。对于采用“网对网” 模式的定点医药机构，其内部网络必须符合等保三级要求，在采用访问控制、数据加密等安全防护措施后才可接入医保专网。原则上单条专线仅供同一地理位置的同一医保编码单位接入，不允许多个不同医保编码单位使用同一专线接入医保专网。

（二）接入方式。各定点医药机构接入医保专网应采用专线或VPDN。其中专线是指运营商提供的裸光纤/MPLS等进行互联的专用线路。VPDN是指运营商基于L2TP/GRE 隧道技术为客户提供的一种可控的4G/5G网络接入方式。对于具有专线接入条件的定点医药机构，选择专线接入医保专网；对于移动终端、自动售药设备以及其他不具备专线接入条件的医保服务场景，可选择VPDN方式接入医保专网。

（三）备用线路。有条件的定点医药机构可依据接入规范要求建设备用线路，该线路可接入到重庆市医保信息平台灾备中心。备用线路可选择不同运营商承建，以确保医保结算的稳定性和可靠性。

二、网络安全建设

（一）专网专用，确保安全隔离。各定点医药机构应采用物理隔离，或部署使用“安全隔离与信息交换系统”的方式，将医保专网与其他网络进行隔离，确保医保专网链路在各种情况下均不可直接连接互联网及其他行业专网。重庆市医保信息平台生产中心为医保业务唯一逻辑汇聚点，各接入单位原则上不进行彼此间医保数据交换。对于手持移动终端以及其他通过无线方式开展医保业务的信息系统，仅可通过由重庆市医保信息平台进行身份认证的VPDN网络接入医保专网。

（二）专机专用，强化终端安全。各定点医药机构应具备相应的保护与防攻击措施，确保医保数据不被篡改和非法获取。其接入医保专网的终端应专机专用，安装终端安全监控和管理软件，不安装来源不明软件，不得一机多网连接，严禁处理涉密信息。 其中终端安全监控和管理软件功能应涵盖病毒查杀、漏洞修复、系统修复、一机多网监测、移动存储介质管理（详见附件）等功能。按照市医保局要求将接入医保专网的终端监控数据统一上传，支持在医保信息平台可视化展示。

三、云HIS接入规范

（一）云HIS基础环境要求。定点医保机构选用云HIS系统对接医保专网的，应要求云HIS服务商采取“专网建云”的模式。**一是自建专有云，**云HIS 服务商可通过自建符合等保三级标准并与互联网及其他行业专网安全隔离的专用云来部署云HIS系统。**二是租用专有云，**云HIS 服务商可依托运营商提供的符合《接入规范》的基础环境部署云HIS系统。

（二）云HIS网络接入。云HIS服务商应保证其服务可覆盖医保专网内所有定点医药机构，在按照基础环境要求完成系统部署后，应采用“网对网”的组网模式，通过专线接入医保专网。

四、工作要求

（一）明晰责任，闭环管理。各定点医药机构对本机构内医保专网、接入终端的数据和网络安全负主体责任，应制定相关安全制度，完善技术防护措施，配备专职操作人员，规范医保结算流程，建立应急处置机制。有条件的定点医药机构应配备专职人员负责医保专网的数据和网络安全。

（二）密切配合，全面整改。各定点医药机构要加强与各运营商、云HIS服务商、技术支持单位的沟通协调，各定点医药机构、云HIS服务商按照通知要求在2024年6月前整改完毕。定点医药机构未按照通知要求进行整改的，严格按《定点医药机构服务协议》相关规定进行处理，云HIS服务商未按照通知要求进行重新部署的，将通知运营商禁止接入医保专网向定点医药机构提供服务。

（三）严防事故，守住安全。各医药机构将网络安全接入、终端安全管理纳入日常管理工作。**一是**要切实做好数据和网络安全防护工作，严防发生重大数据和网络安全事故。对接入医保专网的计算机安装终端安全管理软件，定期进行安全漏洞修复和病毒查杀，定期修改计算机登录密码，防范医保数据滥用和泄露风险。**二是**要定期开展网络安全自查，重点检查“一机多用”、“一机多网”、“专网与互联网混用”等违规行为。

附件：终端安全管理软件（系统/平台）基本功能

重庆市沙坪坝区医疗保障局

2024年3月29日

（联系人：卢秋宇，联系电话：023-65382676）

附件

终端安全管理软件(系统/平台)基本功能

|  |  |  |
| --- | --- | --- |
| **序号** | **功能名称** | **功能要求** |
| 1 | 一机多网监测 | 系统能够识别终端是否同时接入了专网和互联网，如果终端接入了互联网，则系统会自动进行阻断，从而保证终端仅能访问所属的专网，避免机密信息泄露或受到黑客攻击。 |
| 2 | 安全监控 | 系统会对终端的操作行为进行实时监控，对可疑行为进行警报提 示，对异常行为进行记录并进行分析，及时发现威胁并防范潜在的安全风险。 |
| 3 | 软件管理 | 针对终端设备上的软件进行管理，确保软件完整性以及正版授权，禁止未经允许的软件安装，从而避免因非法软件导致的安全风险。 |
| 4 | 补丁推送 | 系统可以收集、分析并推送最新的安全补丁，为终端设备提供安全防护支持，避免因漏洞被攻击导致的信息泄露。 |
| 5 | 病毒查杀 | 系统能够主动扫描终端设备上可能存在的病毒、木马以及其他恶意软件，并进行清除，避免恶意程序对设备造成损害。 |
| 6 | 系统修复 | 系统可以定期自动检查、修复终端设备上的系统问题，确保终端设备的系统稳定性、安全性。 |
| 7 | 恶意软件阻拦 | 系统可以拦截恶意软件、恶意链接等，有效避免由此导致的系统崩溃、数据泄露等安全问题。 |
| 8 | 移动介质管理 | 系统能够限制移动介质(如U盘、移动硬盘)的使用，防止其中的病毒、木马或者其他恶意程序通过移动介质进入终端设备。 |
| 9 | 可视化展示 | 通过可视化方式展示终端设备的安全状态、防护策略，更加方便管理员监控终端设备的安全情况，及时发现安全问题并进行解决。 |

|  |
| --- |
|  重庆市沙坪坝区医疗保障局办公室 2024年3月29日印发 |