成 飞 医 院

管理规章制度

医信专—026—2024

批准：张鹏

信息网络第三方人员安全管理制度

修订记录：

序号	编号	名称	实施日期	修订内容
1	医信专—026—2024	信息网络第三方人员安全管理制度	2024 年 7 月 16 日	新增

第一章 总 则

第一条 制定目的和范围

1、为确保医院的网络信息系统安全，保护患者和医院的信息资产安全，同时根据国家卫生健康委员会医疗质量安全核心制度文件中对网络安全及数据安全要求，规范第三方人员在医院网络环境中的行为，特制定《信息网络第三方人员安全管理制度》（以下简称“本制度”）。

2、本制度适用于所有进入医院信息网络环境的第三方人员，包括但不限于供应商、合作伙伴、顾问、临时访问等。

第二条 职责与范围

1、医院网络环境的访问权限必须经过信息部授权，未经许可，第三方人员不得擅自进入或使用医院的网络信息系统。

2、医院将根据第三方人员的工作需要，为其分配特定的网络访问权限，权限范围包括但不限于访问特定应用程序、数据文件等。

3、第三方人员的权限变更、撤销等操作必须由授权人员进行，并及时更新相关记录。 在授权管理中，应遵循以下原则：最小权限原则：为每个第三方人员分配最小必需的权限，即只授予其完成工作所必需的访问权限，避免过度授权。分层授权：将权限分为不同层次，根据职责和需求分配不同级别的权限，以确保权限的合理分配。周期性审查：定期审查第三方人员的权限，根据其工作变化和情况的需要进行权限调整，避免权限滞留。

4、访问申请和批准流程：第三方人员需要在需要访问医院网络资源时，向信息部人员提交访问申请，以电子（附件 1）申请方式提交指定负责人。授权人员根据审查结果，决定是否批准申请。如果申请合理并符合授权原则，授权人员将批准申请。如果存在问题或风险，可能会拒绝申请或要求申请人提供更多信息。一旦申请被批准，授权人员将根据申请的内容，分配适当的访问权限给第三 方人员。权限的分配应遵循最小权限原则， 确保第三方人员只能访问其工作所需

的资源。授权人员应当及时通知申请人访问权限已经批准，并提供有关如何访问资源 以及注意事项的信息在第三方人员访问资源期间，应设置监控和审计机制，对其访问行为进行实 时监控和记录。这有助于发现异常行为和及时采取措施。

5、授权人员应定期审查第三方人员的访问权限，确保其权限仍然符合实际需求。 如果第三方人员的工作职责发生变化，应及时调整其权限。定义明确的访问申请流程，第三方人员需要向特定的授权人员提出访问请求， 授权人员根据工作需要和权限原则审查和批准请求。当第三方人员的工作任务完成或权限不再需要时，授权人员应及时撤销其访问权限，防止权限滞留的风险。

6、权限审批和记录： 所有权限变更、撤销等操作都应由授权人员进行，且必 须在系统中进行详细记录。这有助于追踪权限变更的历史和目的。临时权限：对于一些需要临时访问的情况，可以考虑授予临时权限，过期 后自动撤销，以减少长期权限的风险。应急权限撤销： 定义应急情况下的权限撤销流程，以确保在发生安全事件 时，可以及时停止第三方人员的访问权限。

第三条 安全意识管理

1、医院将对进入网络环境的第三方人员进行网络安全意识培训，使其了解有关安全政策、规定和操作流程。

2、医院将定期组织网络安全培训，第三方人员有义务参加并完成培训。

3、对于涉及到敏感数据的第三方人员签订附件 2《信息安全保密协议》。

第四条 信息安全和保密措施

1、第三方人员在使用医院网络环境期间，不得窃取、泄露、篡改、毁损医院及 患者的信息资产。

2、在工作完成后，第三方人员应立即登出相关系统，确保未经

授权人员的访问。

3、第三方人员应使用医院提供的设备和工具进行工作，不得私自连接未经授权 的设备或网络。

4、在使用设备时，应定期进行安全更新和杀毒操作，确保设备没有安全漏洞。 不得随意安装、删除软件，不得访问非工作相关的网站和应用。

5、第三方人员应当遵守医院制定的网络安全策略，包括但不限于密码策略、数据备份策略等。

第五条 违规处理

1、一旦发现第三方人员有违反本制度的行为，医院有权立即暂停其网络访问权限，并启动调查程序。

2、根据调查结果，医院将依法采取相应的纠正措施和法律行动。

第二章 附 则

第六条 本制度经医院党委会审议批准。

第七条 本制度自 2024 年 7 月 16 日起施行。

第八条 本制度由信息部编制并负责解释。

附件 1.

成飞医院

第三方远程运维 VPN 及堡垒机账号开通申请表

公司名称（公章）			
责任人（使用人）		联系电话（手机号码）	
身份证号码			
运维对象	主机□ 安全设备□ 应用□		
申请原因： 本人一定遵守国家相关法律法规和成飞医院网络安全相关制度。 责任人（签名）： 日期：			
VPN 账号	**是**□ 否□	**堡垒机账号**	是□ 否□
剪贴板上传文件	是□ 否□	**剪贴板下载文件**	是□ 否□
使用期限	年 月 日至 年 月 日		
医院项目负责人意见： □同意 □不同意 签名： 日期：			

附件 2.

信息安全保密协议书

甲方： 成飞医院

乙方：

驻场工程师： 联系电话：

乙方按照合同要求，派驻公司驻场工程师□常驻/□远程运维成飞医院，协助完成硬件运维、网络安全、信息化建设项目等日常业务，根据《网络安全法》《中华人民共和国保守国家秘密法》《涉密和非涉密网络保密管理制度》《成飞医院医信专—019—2022 信息系统安全管理办法》等相关法律法规和制度签订本保密安全协议：

一、本协议涉及的保密信息内容：

乙方所涉及的院内信息数据包括但不限于人员信息、患者基础数据、财务收入数据、药品信息、诊疗信息等，其信息存在形式包括但不限于书面、计算机磁盘、会议记录、录音录像、电子数据和其他口头形式等。

二、甲方义务

1. 甲方有义务对该项目的乙方人员进行身份及资质审核，落实相关计算机信息安全管理制度。

2. 甲方有义务要求乙方对调取的涉密信息进行安全存放，严防向社会泄露。

3. 甲方有义务对乙方进行相关法律法规、信息安全方面的宣教，使乙方了解并落实相关制度，掌握相关安全防控的知识和技能。

三、乙方保密义务

1. 未经甲方允许患者所有资料不得提供给第三方人员和单位。

2. 未经允许，不查阅、复印甲方数据资料。

3. 不将甲方的患者、员工、收入、药品、材料等资料带出办公场所。

4. 不在不利于保密的地方存放机密文件、院内资料，不将文件、资料乱丢乱放。

5. 不携带涉及保密的材料进行游览、参观、探亲、访友或出入公共场所。不在公共场所或亲朋好友中谈论甲方的相关数据信息。

6. 发现甲方的甲方信息已经泄露或者可能泄露时，应当立即采取补救措施并及时报告甲方以及项目主管负责人。

7.所有数据禁止一切形式的非授权商用。

四、保密期限

乙方在成飞医院项目正常验收完结后 3 年内。

五、违约责任

1. 乙方若违反和甲方相关保密制度，一经发现，视情节轻重，甲方有权利依据相关规定按程序给予乙方交回全部资料、警告、通报批评、承担赔偿责任等处理，并依法追究乙方违约责任，情节特别严重的移交司法部门处理。

2. 由于乙方泄露涉密信息造成医院财产损失、人身伤害、社会不良负面影响等案件发生构成犯罪的，甲方将依法移交司法机关追究刑事责任。

3. 本协议一式贰份，甲、乙双方各执一份，自双方签字且盖章之日起生效。

甲方（章）： 乙方（章）：

法定代表人或授权代表签字： 法定代表人或授权代表签字：

年 月 日 年 月 日