医疗器械安全防护能力技术建议
第一部分：远程运维
（征求意见稿）

目　　次

目　　次 2
前　　言 3
1. 范围 4
2. 规范性引用文件 4
3. 术语和定义 4
4. 适用场景 4
5. 安全防护能力 4
　5.1 通用运维 4
　5.2 远程接入 6
　5.3 器械联网 6
附 录 A 8
附 录 B 9
附 录 C 10
附 录 D 11
附 录 E 12
附 录 F 13
附 录 G 14

前　　言

现阶段智慧医疗场景下多采用远程运维技术。医疗器械远程运维中的安全防护能力，会直接影响网络数据安全的风险和医疗器械的正常运行。本文件将对智慧医疗场景下医疗器械远程运维安全防护能力提出技术建议。

医疗器械安全防护能力技术建议 第一部分：远程运维

1. 范围

本文件提出了智慧医疗场景下医疗卫生机构中医疗器械远程运维安全的通用运维、远程接入和器械联网等方面的技术建议。

2. 规范性引用文件

下列文件对于本文件的宜用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改版）适用于本文件。

GB／T 39837-2021 信息技术 远程运维 技术参考模型 术语和定义

3. 术语和定义

下列术语和定义适用于本文件。

远程运维 remote operation and maintenance

通过信息技术对设备进行远程的数据采集、数据分析、判断设备的运行状态，并提供相宜的运维服务。

4. 适用场景

本文件适用于智慧医疗场景下所使用联网医疗器械远程运维解决方案。

5. 安全防护能力

5.1 通用运维

5.1.1 策略管理

a. 远程运维工作开展前，宜明确远程运维目标和方法，建议形成远程运维策略指导材料；
   - 数据采集声明：宜明确数据采集范围、数据采集方法等要素
   - 远程运维备案书：宜明确远程运维人员信息、远程接入的技术实现方案、安全宜急预案等要素

b. 远程运维工作实施中，宜按照远程运维策略指导材料操作。

5.1.2 账号管理

a. 宜对用户名、口令等个人敏感信息，实施加密等保护措施；
b. 宜明确账号口令的有效周期，账号口令失效前，建议告知用户完成口令更新操作；
c. 宜明确账号口令的复杂度策略，口令宜包含数字、字母及部分特殊符号三种字符；
d. 宜采用一人一账户机制，账户注册时宜绑定个人身份信息。

5.1.3 登录安全

a. 宜明确用户名及口令字符集；
b. 若采用账户手机号绑定策略，宜提供登录失败告知功能；
c. 当多次登录失败时，宜采取图形验证码、锁定账户等安全保护功能。

5.1.4 操作安全

a. 宜采用堡垒机等技术手段实现服务器的安全运维，使得远程运维操作可审查、可溯源；
b. 远程运维人员宜依据前期形成的作业流程进行操作；
c. 宜明确远程运维变更操作的审批流程；
d. 宜提供运维操作超时登出机制并明确超时登出时间等规则。

5.1.5 终端安全

a. 远程接入所使用的终端（统一分配设备、个人设备）宜提供域控策略、防病毒等安全接入能力；
b. 针对软硬件结合的远程运维解决方案，宜提供终端安全能力；
c. 针对只包含软件的远程运维解决方案，宜在产品用户手册等说明性文档中告知终端运维方提供的终端安全能力。

5.1.6 审计安全

5.1.6.1 日志审计

a. 宜提供操作日志的审计能力；
b. 宜明确操作日志的加密保存形式及技术手段；
c. 宜明确操作日志的保存周期。

5.1.6.2 报文审计

a. 宜提供通信报文的审计能力；
b. 宜采取不同通信协议所需审计的报文内容（使用 http/https/ssh 协议，宜提供审计完整的明文通信传输内容的能力，使用 ftp 协议传输文件，宜提供审计传输的时间、文件名称，文件大小等内容的能力）；
c. 宜明确通信报文的加密保存形式及技术手段；
d. 宜明确通信报文的保存周期。

5.1.6.3 录屏审计

a. 宜提供运维操作录屏的审计能力；
b. 宜明确录屏视频文件的加密保存形式及技术手段；
c. 宜明确录屏视频文件的保存周期。

5.1.7 监管安全

5.1.7.1 安全监督

a. 宜采用录屏技术手段记录远程运维人员的操作；
b. 宜提供抓取远程运维操作通信报文的能力；
c. 针对涉及个人重要信息等高度敏感操作，宜通过采取视频监控模式进行监管；
d. 针对远程运维人员的高危操作，监管人员宜提供切断网络连接的能力。

5.1.7.2 安全组织

a. 宜明确负责远程运维安全的职能部门及相关负责人；

b. 宜明确远程运维人员的工作职责和能力，宜对核心操作人员开展背景调查等资质审核工作；
c. 宜定期组织开展安全培训。

5.1.7.3 安全考核

a. 宜明确远程运维安全管理制度和考核机制；
b. 宜定期开展风险评估、漏洞扫描等安全自查工作。

5.1.8 数据安全

5.1.8.1 数据存储能力

a. 宜建立数据存储安全的制度规范；
b. 宜提供存储介质、逻辑存储空间的安全管理能力。

5.1.8.2 数据使用能力

a. 宜建立数据使用安全的制度规范；
b. 宜明确数据使用权限申请审核流程。

5.1.8.3 数据销毁能力

a. 宜建立数据销毁和存储介质销毁方案；
b. 宜提供数据销毁记录审计能力。

5.2 远程接入

5.2.1 虚拟专用网络（VPN）接入

详见附录 A

5.2.2 虚拟桌面基础架构（VDI）接入

详见附录 B

5.2.3 端口映射接入

详见附录 C

5.2.4 基于计算机图形界面图像压缩技术接入

详见附录 D

5.3 器械联网

若远程运维解决方案涉及联网医疗设备，需参考本章节。

5.3.1 无线网络接入

5.3.1.1 Wi-Fi（IEEE 802.11）接入

详见附录 E

5.3.1.2 4G/5G（LTE）接入

详见附录 F

5.3.1.3 物联网（射频识别）接入

详见附录 G

5.3.2 有线网络接入

同通用运维。

附 录 A
（规范性附录）

虚拟专用网络（VPN）接入

a. 宜提供接入终端的安全管控能力；
b. 针对不同的业务场景，宜提供不同的身份认证方式；
c. 宜提供数据传输加密能力；
d. 宜符合国家密码硬件的相关规范；
e. 宜支持国密算法等安全加密算法。

附 录 B
（规范性附录）

虚拟桌面基础架构（VDI）接入

a. 宜提供对异地接入终端的安全检查能力；
b. 宜采用虚拟局域网等技术手段，实现内部子网的物理隔离；
c. 宜关闭常见病毒使用的端口；
d. 宜采用白名单等技术手段，对远程接入操作行为进行安全控制和规范；
e. 针对核心场所或关键部位，宜采用虚拟化技术净化终端操作系统环境，从而提高系统的的安全性；
f. 宜提供访问控制能力，包括状态包过滤、宜用级过滤、防 DDos 攻击等安全防护能力。

附 录 C
（规范性附录）

端口映射接入

a. 宜在本地服务器内部署防火墙等安全防护产品；
b. 宜定期对内部资源和系统开展安全自查，包括宜用漏洞扫描、源代码检测、安全风险评估等。

附 录 D
（规范性附录）
基于计算机图形界面图像压缩技术接入

a. 宜采用物理网络隔离技术；
b. 宜采用从外网到内网单向鼠标键盘信号输入方式；
c. 宜采用从内网到外网单向显示信号输出。

附 录 E
（规范性附录）
Wi-Fi（IEEE 802.11）接入

a. 针对重要系统，宜采用电磁屏蔽等技术手段；
b. 宜定期采取站点检查，以及时发现未被授权的网络；
c. 宜提供无线网络健康状态的监测能力；
d. 针对传输敏感数据的业务场景，宜采用 SSH、SSL、IPSec 等加密技术。

附 录 F
（规范性附录）
4G/5G（LTE）接入

a. 宜提供网络域的双向认证能力；
b. 宜提供多重信息认证能力；
c. 宜定期对系统开展安全加固工作；
d. 宜提供端到端、多层次资源的安全隔离能力；
e. 宜提供对关键数据进行加密和备份操作能力；
f. 宜提供对开源第三方软件的安全管理能力；
g. 宜提供可使用云化、虚拟化隔离措施等技术手段；
h. 宜提供对边缘计算设施的物理保护和网络防护能力；
i. 宜提供对网络安全威胁监测与处置能力；
j. 宜提供网络开放接口的安全防护能力。

附 录 G
（规范性附录）
物联网（射频识别）接入

a. 宜采用密码认证、密钥散列消息认证码、数字签名等身份认证技术；
b. 宜提供覆盖编码能力；
c. 宜提供电磁屏蔽等技术手段；
d. 宜采用各种无线电频率通信（包括低频、高频、超高频、微波波段）；
e. 宜提供读写器定期查询标签能力；
f. 宜提供保护标签的技术能力。