2020数字医疗

疫情防控期间网络安全风险研究报告

CAICT 中国信通院

中国信息通信研究院安全研究所

卫生信息安全与新技术应用专业委员会

数据保护官（DPO）社群

2020.03

六、疫情期间网络安全工作思路建议

（一）强化安全标准，规范行业发展

健康医疗行业网络安全标准化工作是健康医疗领域网络安全保障体系建设的重要组成部分,在推动健康医疗领域网络安全治理体系变革方面发挥着不可替代的作用。安全标准体系的制定、完善和落地，有助于规范和推动医疗信息化、医疗App及医疗设备等全医疗领域数字化的安全建设。随着物联网、5G等新技术在数字医疗领域的深度应用，新型医疗设备和医疗应用不断涌现，亟需健全完善的健康医疗行业网络安全标准化体系建设。应充分利用ICT领域新技术安全应用实践经验，支撑和构建新型医疗设备和医疗应用等领域的安全标准体系，推动数字医疗与ICT融合领域安全发展。

（二）持续动态监测，建立反馈闭环

网络安全风险具有长期性和动态变化的特点，且不同行业的网络安全风险特点不同。因此，建立健康医疗行业维度的网络安全风险观测机制和平台十分重要。与此同时，风险动态监测需要与风险反馈处置形成闭环，将监测到的安全风险尽快反馈到存在风险的医疗机构，修复相关安全漏洞或升级相关服务版本，从而有效控制和降低健康医疗行业整体的安全风险。

（三）加强安全培训，提高安全意识

相关人员网络安全意识不足是健康医疗行业面临的重大安全挑战。实际上，在安全观测中发现的数据服务暴露、组件版本过低以及高危端口开放等安全隐患，都直接或间接与人员网络安全意识不足存在关联。应推动和加强健康医疗行业从业人员网络安全相关培训，建立健全医疗机构内部网络安全管理规章制度，从医疗信息系统安全设计研发维护、医疗设备安全操作运维管理、医疗数据安全采集存储共享等多方面、全视角规范内部安全操作流程，切实提升相关人员的网络安全意识，落实网络安全责任。

（四）突出能力建设，形成长效机制

健康医疗行业相关机构应提升自身网络数据安全综合防护能力，加强在网络数据安全领域的投入，建立系统化的安全保障体系，构建安全长效机制：

- 加快推进网络安全等级保护测评工作，定位安全问题，排除安全隐患。
- 定期开展网络安全风险评估工作，评估医疗设备、医疗信息系统安全状况，发现潜在的安全风险。
- 协同国家专业安全机构，建立新型医疗设备和技术的安全融合应用机制，保障数字医疗新技术的安全发展。

中国信息通信研究院 安全研究所

地址：北京市海淀区花园北路 52 号

邮政编码：100191

联系电话：18610049972

电子邮箱：guofei@caict.ac.cn, zhangxueyang@caict.ac.cn

传真：010-62300264

网址：www.caict.ac.cn