《医疗卫生机构网络安全管理办法》的政策解读

发布时间： 2022-08-30 来源: 规划发展与信息化司

随着高质量发展纵深推进，全国卫生健康领域迎来重要机遇期，信息化发挥着关键的支撑作用，在此过程中产生的医疗健康数据不仅是重要的生产要素，更是国家基础性战略资源，因此网络安全的重要性日益凸显。在此背景下，《医疗卫生机构网络安全管理办法》（以下简称《办法》）的发布，进一步规范了医疗卫生机构网络和数据安全管理、促进“互联网+医疗健康”发展，加快推动卫生健康行业高质量发展进程。

《办法》明确了各医疗卫生机构网络及数据安全管理基本原则、管理分工、执行标准、监督及处罚要求，体现了统筹安全与发展的总体平衡，与此前出台的一系列政策法规一脉相承，为医疗卫生机构指明了网络安全管理的总方向，主要体现在以下四个方面：

一、强调一个周期。《办法》全文贯穿了全生命周期管理的主导思想。在网络安全方面，围绕信息系统全生命周期，提出落实等级保护制度、监测预警、应急实战、安全整改、人员管理、新技术应用、密码安全、医疗设备、供应链管理等方面的要求；在数据安全方面，以保障数据的机密性、完整性、可用性为目标，要求采取数据加密、数据备份、数据脱敏等技术，加强数据收集、传输、存储、使用、交换、销毁等全生命周期的安全防护。在实际运用中，应基于网络和数据的全生命周期视角，梳理安全策略架构,识别具体业务场景，有针对性的设计安全措施，实现安全防护。

二、突出两个要点。《办法》强调医疗卫生机构安全管理应围绕顶层设计和制度保障两个要点着力推进。顶层设计方面，在整体网络安全体系的基础上，依据数据的特性建构网络和数据安全顶层设计，落实安全责任分工，明确数据管理部门、业务部门、信息化部门在网络和数据安全管理工作中的权责。制度保障方面，《办法》明确医疗卫生机构应建立健全安全管理制度、操作规程及技术规范。在执行过程中，应密切结合自身业务模式的变更，及时修订完善制度要求，保持网络和数据安全制度的有效执行力及充分协同。

三、融合三位一体。《办法》要求建立网络安全管理制度体系，加强网络安全防护，通过管理和技术手段保障数据安全和数据应用的有效平衡。在实际运用中，应将总体安全策略拆解到具体安全管理要求，并通过安全技术实现管理要求，最终融入对应到安全运营体系中，形成融合管理、技术、运营三位一体的立体化网络安全管理模式。

四、构建四个体系。《办法》指出要建立防护、监测、处置、保障四个体系协同的综合防控格局。在安全防护方面，要求建立“实战化、体系化、常态化”的安全防护体系，形成“动态防御、主动防御、纵深防御、精准防御、整体防控、联防联控”的安全防护态势；在安全监测层面，鼓励三级医院探索态势感知平台建设，及时收集、汇总、分析各方网络安全信息，并与国家及行业平台对接；在安全处置方面，要形成监督管理、安全检查、应急预案、联防联控协同体系；在安全保障方面，通过统筹领导和规划设计，在人才培养、安全培训、经费支持等方面实现全方位保障。

总体而言，《办法》坚持安全可控和开放创新并重的基本原则，其颁布为医疗卫生机构网络安全管理提供了工作指南，筑牢了医疗卫生机构安全屏障，奠定了卫生健康行业网络安全发展基础。

相关链接：关于印发医疗卫生机构网络安全管理办法的通知