重庆市卫生健康委员会
关于印发《重庆市卫生健康行业网络安全工作规范》的通知

渝卫发〔2019〕66号

各区县（自治县）卫生健康委、两江新区社发局、万盛经开区卫生计生局，各委属（代管）单位，委机关各处室：

经委主任会讨论通过，现将《重庆市卫生健康行业网络安全工作规范》印发给你们，请遵照执行。

重庆市卫生健康委员会

2019年12月18日

重庆市卫生健康委员会发布

重庆市卫生健康行业网络安全工作规范

随着信息化的快速发展和信息技术的广泛应用，网络安全面临的威胁持续加大，卫生健康行业网络安全工作关系着本行业信息化的稳步推进和医疗卫生事业的改革发展。为深入贯彻中央和市委关于网络安全工作的总体部署，加快建立健全医疗卫生行业网络安全保障体系，提高防护能力和水平，保障医疗卫生行业信息化建设健康有序地发展，依据《中华人民共和国网络安全法》和国家网络安全等级保护 2.0 等相关规定，经重庆市卫生健康委员会网络安全与信息化建设领导小组同意，制定本规范。

一、总体要求

以提升卫生健康行业网络安全保障能力为主线，以完善网络安全保障体系为目标，全面提高网络安全意识，建立健全行业网络安全工作的组织体系、管理规章和责任制度，落实国家信息安全等级保护制度，着力提高网络基础设施、业务系统和关键信息基础设施安全防护水平，增强卫生健康行业网络安全技术能力，强化信息数据保护，推进行业内安全可控关键软硬件应用，有效

重庆市卫生健康委员会发布

防范、控制和抵御信息安全风险，增强安全预警、应急处置和灾难恢复能力，为我市卫生健康事业发展提供网络信息安全保障。

二、适用范围

本规范适用于重庆市卫生健康行业内各级各类卫生健康行政部门、事业单位、医疗卫生机构、提供卫生健康技术支撑及服务运维机构。

三、基本原则

坚持依法治理的原则，严格遵照国家和重庆各项网络安全法律法规、政策规范；坚持网络安全与信息化发展并重的原则，统一谋划、统一部署、统一推进、统一实施；坚持预防为主的原则，做好隐患排查治理，确保行业网络信息运行安全。

四、工作任务

（一）完善组织体系，明确责任分工

1. 市-区县两级卫生健康行政部门应建立网络安全和信息化建设工作领导小组，负责统筹辖区内卫生健康行业网络安全工作。

2. 各单位要建立党政一把手负责的统筹网络安全与信息化工作的领导机构，主要负责人是网络安全的第一责任人。同时根据单位实际，应设立或明确职能部门和专职人员管理本单位网络

安全与信息化工作，做到定岗定责，专人专管。每年至少召开一次主要负责人参加的专题网络信息安全会议。建立健全内部管理协调机制，建立联结各级政府网络安全主管部门、卫生健康行业行政主管部门和主体责任单位的跨部门协调处理机制，充分发挥纵向链接、横向协调的组织保障作用。

3.各单位按照“谁主管谁负责、谁运营谁负责、谁使用谁负责”和“分级管理”的原则落实网络安全责任。

（1）监管责任。市-区县两级卫生健康行政部门对辖区内本行业网络安全负监管责任，主要负责：统筹辖区内行业网络安全体系建设；落实行业网络安全政策法规和标准规范，制定具体工作细则，组织开展行业网络安全政策及技能培训，指导辖区内各单位开展网络安全工作；建立评价与考核机制，每年至少开展一次辖区内行业网络安全检查，督促落实网络安全责任、保障网络安全经费并做到经费专款专用。

（2）主体责任。市卫生健康行业内所有单位对本单位的网络安全负主体责任，主要负责：建立健全本单位网络安全保障体系和工作责任体系，落实卫生健康行业网络安全相关政策和标准规范；本单位职能范围内管理及建设的网络与系统安全工作；制定并落实相应管理制度，做好隐患排查整改，确保网络与数据安

全。

（3）直接责任。依法取得辖区卫生健康行政部门和建设单位授权或委托的情况下提供技术支撑及服务运维的机构、团队、企业及个人等承担网络安全的直接责任，主要负责：承担授权或委托范围内相关软硬件建设运维、安全保障和日常管理等技术服务工作，负责所涉系统及数据的隐患排查、安全整改和应急处置等工作；对涉及数据承担安全保护和保密责任；接受本级网络安全主管部门、卫生健康行政部门和建设单位的管理、指导、监督。

（二）做好统筹规划，建设管理并行

4.各单位对网络安全工作要统一管理，按照“同步规划、同步建设、同步管理”原则，做好统筹规划，将网络安全工作融入信息化整体建设和管理中。

（1）必须建立本单位、本辖区的短、长期安全规划，每年制定年度网络安全工作计划，编制资金预算计划，结合整体信息化建设同步投入，开展本单位网络安全防护体系建设，切实做到内容与技术并重、建设与管理并行。

（2）在网络与信息系统可研及设计阶段，应全面分析网络安全风险，编制网络安全防护方案。按照网络安全等级保护 2.0 要求开展等级保护定级，同时向本级卫生健康行政部门报备。对

于定级在等级保护三级及以上的系统，网络安全防护方案的合法性、完整性、针对性、科学性应当进行评审，形成评审意见后报市卫生健康行政部门备案。

（3）在网络与信息系统研发阶段，采用的开发平台、开发工具、第三方软件等应有正版授权，编写的代码应符合安全规范；所购买的网络安全产品、服务应符合相关国家标准的强制性要求，优先应用自主可控数据安全产品，支持国产密码算法的数据安全产品应用推广。

5.各级卫生健康行政部门依法对辖区内行业机构网络安全工作进行监督检查。检查的方式主要有抽查、询问、查询以及技术检查等方式。技术检查采用漏洞扫描、渗透测试等方式进行。

（三）建立健全制度，强化运行管理

6.各单位要按照国家有关网络安全的政策要求，结合自身实际，加强安全管理研究，合理制定辖区或单位内的各种信息安全制度、规范、流程。主要包括：网络安全总体策略方针、网络安全组织架构、各项管理制度、流程以及对应的表单等。

（1）制定和落实网络安全基线规范，确保网络、主机、应用、数据、管理等各个方面满足安全基线要求。

（2）建立实时监测与威胁情报检查机制，落实网络安全监

测预警工作。采取网络安全监测手段，对网络设备、网络流量、网络内容、网络攻击等进行监测，加强对大数据、云计算等新技术新应用的监测。

（3）加强安全审计工作，实现对主机、数据库、中间件、业务应用等安全审计和安全运维审计，记录网络与信息系统运行状态、安全事件，留存相关日志不少于六个月。

（4）制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；建立网络安全应急机制，做好应急保障工作，每年至少开展一次网络安全应急演练，并将演练情况报送本级卫生健康行政部门。

（5）系统下线应进行全面评估，确认系统下线后的残留风险以及是否对其它系统造成影响，下线后应撤销等级保护备案，做好数据擦除工作。

（6）严格落实网络安全岗位要求，录用的网络安全管理、技术等重要岗位从业人员的背景应进行严格审查，确保无违法犯罪行为记录。

（7）网络安全岗位人员发生调动、离职等工作变化时，应在调动（离职）前收回相关访问权限并签署保密协议，调动（离职）后 10 个工作日内应修改原岗位人员所有账号口令。

（8）应加强对于合作或技术支撑单位安全责任管理，系统建设单位应与其签订保密协议，应做好其开发运维人员情况、操作记录的监测。合作单位或个人发生人员变动、岗位调整等情况时应主动通告系统建设单位，并按前条规定做好相应工作。

（9）每年将年度网络安全工作开展情况报本级卫生健康行政部门。

（四）依托等保制度，加强测试测评

7.各单位应对本单位各信息系统做好安全测试与等级保护测评管理工作。

（1）在信息系统开发过程中应同步开展代码安全检查和安全风险评估测试工作。信息系统上线前应通过具有网络安全风险评估资质的第三方网络安全服务机构测试，并完成系统的定级、备案、测评、整改工作。等级保护三级以上系统的测试报告、测评和整改情况应报市卫生健康行政部门备案。

（2）定期组织开展网络安全等级保护测评和整改工作，等级保护测评机构应具有国家网络安全等级保护管理机构的推荐资质，从事等级测评的人员应具有等级测评师资质。二级系统每两年至少进行一次等级测评，三级系统每年至少进行一次等级测评和安全风险评估。每年年底将等级保护工作开展情况报本级卫

生健康行政部门。

（五）严格数据管理，确保信息安全

8.各单位负责本辖区、本单位各类信息数据的管理工作，主要承担以下任务：

（1）按照相关法律、法规建立健全用户个人信息保护制度，落实《重庆市政务数据资源管理暂行办法》、《重庆市卫生健康行业健康医疗数据资源管理办法》，确保用户个人信息在收集、使用、保存、传输、发布过程中的安全。

（2）采取权限控制、安全加密、安全审计、数据脱敏等技术措施，确保数据在产生、收集、传输、存储、处理、销毁等全环节的安全。

（3）按照数据重要程度分类，明确备份及恢复策略，严格控制数据备份和恢复过程，对重要数据进行容灾备份。原则上我市卫生健康行业生产数据应在市内存储。

（4）建立健全数据安全监测、审计机制及相关技防措施，提高对各类网络泄密事件的发现、处置、溯源能力。

（六）落实通报规范，建立通报机制

9.我市卫生健康系统网络安全信息通报工作按照《重庆市卫生健康系统网络与信息安全信息通报工作规范》，各单位应依据

规范建立本辖区、单位内部的通报机制，与网信、公安、工信以及网络运营商等单位建立常态化的应急协调处置机制，完善人员与联系渠道，建立重大网络安全事件处置和报告制度，确定报送范围、规范报告格式、建立报送流程、明确报送时间。卫生健康行业其他单位参照执行。

（七）建立应急预案，优化处置流程

10.各单位应制定网络安全应急预案，明确应急处置流程和权限，落实应急处置技术支撑队伍，开展安全应急演练，提高网络安全应急处置能力。

（1） 发生安全事件后，应当立即采取措施降低损害程度，防止事件扩大，保存相关记录；按照应急处置程序立即向有关部门报告，做到处置迅速、报告及时。

（2） 辖区内发生重要信息系统崩溃、数据丢失泄漏、大规模病毒感染和网络攻击等重大安全事件，以及出现网信、公安、保密等安全主管部门检测并通报相关事件时，区县卫生健康行政部门应第一时间上报市卫生健康委，市卫生健康委依据应急预案按严重程度成立市级应急处置工作组督促指导事件主体责任单位开展应急处置，市卫生健康统计信息中心提供技术支撑。

（八）重视队伍建设，丰富培训内容

11.各单位应选拔具有网络和信息系统管理经验和专业技能的人员从事网络安全管理工作，有条件的单位应建立网络安全管理专职队伍和技术支撑专业队伍，落实岗位责任和奖惩考核机制。

12.各单位应制定网络安全的培训规划，开展面向全员的普及性培训，加强管理和技术人员的专业培训。每年组织网络安全岗位人员进行网络安全政策、规范、意识、技能等方面的专业培训不少于一次，培训可采用内部培训、外部培训等方式。鼓励联合网信、公安等安全主管部门以及第三方网络安全服务供应商建立多种形式的人才培养体系。

本规范从2020年1月20日开始施行。