焦作市卫生健康委员会文件

焦卫规信〔2022〕2号

转发河南省卫生健康委关于落实网络安全等级保护制度完善行业网络安全综合防控体系的意见

各县（市、区）卫生健康委、市直医疗卫生单位、焦煤集团中央医院：

现将《河南省卫生健康委关于落实网络安全等级保护制度完善行业网络安全综合防控体系的意见》转发你们，请按要求做好相关工作。

2022年3月22日

河南省卫生健康委关于落实网络安全等级保护制度完善行业网络安全综合防控体系的意见

各省辖市、济源示范区卫生健康委、南阳市中医药管理局，省直医疗卫生单位:

网络安全等级保护制度是《网络安全法》确定的基本制度。做好网络安全等级保护工作，对于促进全省卫生健康行业信息化健康发展，服务医药卫生体制改革，维护社会公共利益、社会秩序和国家安全具有重要意义。为深入贯彻落实网络安全等级保护制度，健全完善行业网络安全综合防控体系，有效防范网络安全威胁，有力处置网络安全事件，切实保障全省卫生健康行业网络安全，特制定本意见。

一、指导思想

以习近平新时代中国特色社会主义思想为指导，按照党中央、国务院决策部署，以总体国家安全观为统领，认真贯彻实施网络强国战略，全面加强网络安全工作统筹规划，以贯彻落实网络安全等级保护制度为基础，以保护重要网络和数据安全为重点，全面加强网络安全防范管理、监测预警、应急处置等各项工作，及时监测、处置网络安全风险、威胁和网络安全突发事件保护重要网络和数据免受攻击、侵入、干扰和破坏，切实提高网络安全保护能力，维护国家安全和社会公共利益，保护人民群众的

合法权益，保障和促进全省卫生健康行业信息化健康发展。

二、基本原则

（一）遵循标准、重点保护。严格执行国家网络安全法律法规、政策和标准规范，根据网络（包含网络设施、信息系统、数据资源等）在国家安全、经济建设、社会生活中的重要程度，以及其遭到破坏后的危害程度等因素，科学确定网络的安全保护等级，重点保障第三级（含第三级、下同）以上网络的安全。

（二）行业指导、逐级负责。卫生健康部门履行本行业网络安全主管、监管责任，行业网络运营者履行主体责任，按照“谁主管谁负责，谁运营谁负责”的原则，协调配合、群策群力，形成工作合力。

（三）同步建设、综合防护。坚持网络安全归口管理，统筹谋划，与信息化工作同步规划、同步建设、同步使用。新建网络应在规划设计阶段确定安全保护等级，对于已投入运行且尚未定级的网络，要及时完成定级，确保有序推进后续的安全建设、等级测评、整改加固等相关工作，防范重大网络安全风险、事件发生。

三、工作目标

（一）网络安全等级保护制度深入贯彻实施。网络安全等级保护定级备案、等级测评、安全建设和检查等基础工作深入推进。网络安全保护“实战化、体系化、常态化”和“动态防御、主动防

御、纵深防御、精准防护、整体防控、联防联控”的“三化六防”措施得到有效落实，行业网络安全综合防控能力和水平显著提升。

（二）网络安全监测预警和应急处置能力显著提升。跨单位、跨地区的网络安全监测体系和网络安全保护平台基本建成，网络安全态势感知、通报预警和事件发现处置能力明显提高。网络安全预案科学齐备，应急处置机制完善，应急演练常态化开展，网络安全重大事件得到有效防范和处置。

（三）行业网络安全综合防控体系基本形成。网络安全保护工作机制健全完善，卫生健康行业、公安机关指导，各级各部门分工负责，社会力量多方参与的网络安全工作格局进一步完善。网络安全责任制得到有效落实，网络安全管理防范、监督指导等能力显著提升，行业网络安全综合防控体系基本形成。

四、工作任务

（一）依法落实网络安全等级保护制度

1.深化定级备案工作。各级卫生健康行政部门、网络运营者应全面梳理本单位各类网络，依据《网络安全等级保护定级指南》科学确定网络的安全保护等级。第二级以上网络依法向公安机关备案，并向行业主管部门报备。以下网络安全保护等级原则上不低于第三级：

（1）卫生健康统计数据直报、传染性疾病报告、卫生监督

信息报告、突发公共卫生事件应急指挥信息等跨地区、跨部门联网运行的省级业务信息系统；

（2）省、市、县全民健康信息平台；

（3）涉及大量公民个人信息以及为公民提供公共服务的业务数据中心、大数据平台或系统；

（4）三级医院的核心业务信息系统（包含 HIS、EMRS、PACS、LIS、重症、供应室等各个业务系统的组合）及平台；

（5）其它重要的网站、信息系统和数据。

2.主动开展等级测评。网络运营者应依据有关标准规范，对已定级备案网络的安全性进行检测评估，查找可能存在的网络安全问题和隐患。第三级以上网络每年开展一次网络安全等级测评，并及时将等级测评报告提交受理备案的公安机关和行业主管部门。新建第三级以上网络应在通过等级测评后投入运行。网络运营者在开展测评服务过程中要与测评机构签署安全保密协议，并对测评过程进行监督管理。

3.科学开展安全建设整改。依据相关国家标准，全面梳理分析网络安全保护需求，结合等级测评过程中发现的问题隐患，按照“一个中心（安全管理中心）、三重防护（安全通信网络、安全区域边界、安全计算环境）”的要求，认真开展网络安全建设和整改加固，全面落实安全保护技术措施。要采购安全可信的网络产品和服务，确保供应链安全。网络运营者可将网络迁移上云，

或将网络安全服务外包，充分利用云服务商和网络安全服务商提升网络安全保护能力和水平。

4.落实密码安全防护要求。贯彻落实《密码法》等有关法律法规规定和密码应用相关标准规范，推进国产密码在安全体系中的应用。第三级以上网络应正确、有效采用密码技术进行保护，并使用符合相关要求的密码产品和服务。第三级以上网络运营者应在网络规划、建设和运行阶段，按照密码应用安全性评估管理办法和相关标准，在网络安全等级测评中同步开展密码应用安全性评估。

（二）协作推进行业网络安全综合防控体系建设

1.建立健全工作机制。建立部门联动工作机制，定期与公安等部门召开联席会议，协作开展安全监测、通报预警、应急处置、情报信息等工作，提升应对、处置网络安全突发事件和重大风险防控能力。健全网络安全信息共享通报预警机制，加强本行业、本领域网络安全信息通报预警力量建设，及时收集、汇总、分析各方网络安全信息，组织开展网络安全威胁分析和态势研判，及时通报预警和处置。完善网络安全应急响应处置机制。各级行业主管部门按照国家有关要求制定网络安全应急预案，按照“第一时间发现、第一时间处置、第一时间调查和第一时间整改”的原则，建立网络安全事件报告制度和应急处置机制，在处置的同时及时向公安机关报告。

2.积极主动防范管理。强化网络安全监测、态势感知、通报预警和应急处置等重点工作，保护云计算、物联网、新型互联网、大数据、智能医疗设备等新技术新应用新业态安全。**建设行业网络安全管理平台，**建立智慧大脑系统，依托平台和大数据开展实时监测、通报预警、应急处置、安全防护、指挥调度等工作。**建设行业网络安全监控指挥中心，**对重要网络等开展实时监测，发现网络攻击和安全威胁，立即报告公安机关和有关部门并采取有效措施处置，着力防范重大网络安全风险。**建设行业等级保护定级备案数据库，**开展等级保护备案情况清查建档活动，在等级保护定级备案、检测评估，网络规划建设，以及关键岗位人员管理、供应链管理、应急处置等重点环节实现数字化，实时监测管理。

3.加大网络安全重点环节治理。保障健康医疗数据安全。贯彻《健康医疗数据安全指南》要求，建立并落实重要数据和个人信息安全保护制度，采取关键技术措施，保护重要数据全生命周期安全，确保数据的完整性、保密性和可用性;明确数据安全责任，确保数据使用和披露的合法合规性，保护个人信息安全、社会公众利益和国家安全;强化数据的公有属性，严禁系统承建厂商以任何借口利用数据谋取不正当利益，确保在符合安全要求的前提下满足业务发展需求，规范和推动健康医疗数据的整合共享、开放应用。**加强对网站、APP 等的监测预警。**依据职能，对全省卫生健康行业已有的网络、网站、APP 进行常态监测并实

时管控，开展风险评估，排查苗头性问题，对可能发生的安全问题进行预警和及时处置，着力防范重大网络安全风险。**完善信息上报反馈制度。**第三级以上网络运营者应及时接收、处置来自国家、行业和地方网络安全预警通报信息，按规定向行业主管部门、备案公安机关报送网络安全监测预警信息和网络安全事件。发现严重网络攻击和安全威胁，要立即报告省卫生健康委，并采取有效措施处置，提升行业网络安全监测、预警、通报、响应能力。

4.加强网络安全问题隐患整改督办。对全省卫生健康行业运营单位网络安全工作不力、重大安全问题隐患久拖不改，或存在较大网络安全风险、发生重大网络安全事件的，按照规定的权限和程序，会同公安机关对相关负责人进行约谈，挂牌督办。网络运营者应按照有关要求采取措施，及时进行整改，消除重大风险隐患。发生重大网络安全案事件的，省卫生健康委网络安全和信息化领导小组将组织全行业开展整改整顿。

（三）全面细化落实网络安全责任

1.明确安全保护工作责任。依据《网络安全法》等法律法规和有关政策要求，按照“谁主管谁负责、谁运营谁负责”的 加固原则、厘清网络安全保护边界，明确安全保护工作责任，做到“守土有责、守土尽责”。县级以上卫生健康行政部门对本行政区域内卫生健康行业的网络信息与数据安全负指导监管责任，各级各类医疗卫生机构履行网络信息与数据安全保护义务，对职责范围

内的网络信息与数据安全承担主体责任，网络与信息系统的运行维护部门承担系统的技术安全保障责任，网络与信息系统的使用单位和个人承担系统操作与信息内容的直接安全责任。

2.完善网络安全工作责任制。全省各级卫生健康行政部门和各级各类医疗卫生机构依照法律法规的规定和相关标准，建立“主要负责人负总责，分管负责人牵头抓”的网络安全工作责任制。建立健全内部管理协调机制，与各级政府网络安全管理部门、公安机关建立跨部门协调和安全事件处理机制，充分发挥纵向衔接、横向协调的组织保障作用。

3.加强网络安全监督检查。组织开展网络安全自查和检测评估，以防攻击、防入侵、防篡改、防窃密为重点，深入查找网络安全风险隐患并强化整改，提升行业网络安全防护能力和水平。组织网络安全专项检查，坚持以查促建、以查促管、以查促防、以查促改，每年至少组织一次网络安全工作检查，特殊时期及时检查。组织应急演练，积极探索与公安机关联合开展应急演练，排查苗头性问题，不断提升安全保护能力和对抗能力。整改加固应急演练中发现的突出问题和漏洞隐患，完善保护措施。

4.落实责任追究制度。各级卫生健康行政部门和各级各类医疗卫生机构有关人员违反或未能正确履行网络信息与数据安全职责，按照《网络安全法》、公安部《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》（公安部

1960号文）以及国家卫生健康委《关于落实卫生健康行业网络信息与数据安全责任的通知》（国卫办规划函〔2019〕8号）等系列法律法规、政策要求，严格追究其相关责任，对存在违法行为的，由公安机关依法进行行政处罚，构成犯罪的依法追究刑事责任。

五、保障措施

（一）加强组织领导。各单位要高度重视网络安全等级保护和网络安全综合防控体系建设工作，将其列入重要议事日程，加强统筹领导和规划设计，积极协调把卫生健康核心数据、重要信息系统、重大信息化基础设施等纳入本地网络与信息安全的保障范围。各级卫生健康行政部门和网络运营者要明确本单位主要负责人是网络安全的第一责任人，并确定一名领导班子成员分管网络安全工作，成立网络安全专门机构，明确任务分工，一级抓一级，层层抓落实。

（二）加强网络安全经费保障。各单位要通过现有经费渠道，保障第三级以上网络等开展等级测评、风险评估、密码应用安全性检测、演练竞赛、安全建设整改、安全保护平台建设、密码保障系统建设、运行维护、监督检查、教育培训等经费投入，支持网络安全技术研究开发和创新应用。

（三）严格监管考核。各单位要进一步健全完善网络安全考核评价制度，明确考核指标，组织开展考核。在医疗机构等级评

审中，要严把网络安全关，做好事前审查，事中检查，事后追（问）责。有条件的单位要将考核与绩效挂钩。对卫生健康网络信息安全工作成果突出的单位和个人适时总结，通报表扬。

（四）创新完善人才保障机制。探索成立“产、学、研”一体化的网络安全联合实验室，加强行业网络安全技术交流，引进高层次网络安全人才和先进技术。开展安全培训，提高网络安全意识，提升安全防范技能。适时组织岗位练兵活动，发现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，有条件的可引入可信的专业网络信息安全服务，提升应对能力。

（信息公开形式:不予公开）

焦作市卫生健康委员会办公室　　2020年3月22日印发