# 开封市医疗保障局文件

汴医保〔2020〕104号

## 关于印发《开封市医疗保障局网络与信息安全事件应急预案》的通知

各县（区）医保局、城乡一体化示范区人社局，市医保中心：

为提高处理突发网络与信息安全事件的能力，形成科学、有效、反应迅速的应急工作机制，开封市医疗保障局制定了《开封市医疗保障局网络与信息安全事件应急预案》，现印发给你们，请遵照执行。

开封市医疗保障局 4102010110364

2020年10月19日

# 开封市医疗保障局
# 网络与信息安全事件应急预案

## 一、总则

### （一）目的

为提高开封市医疗保障局（以下简称医保局）处理突发网络与信息安全事件的能力，形成科学、有效、反应迅速的应急工作机制，确保重要计算机信息系统的实体安全、运行安全和数据安全，最大限度地减少网络与信息安全突发公共事件的危害，保护公众利益，特制定本预案。

### （二）适用范围

本预案适用于医保局发生和可能发生的网络与信息安全突发事件。

### （三）工作原则

1.预防为主。立足安全防护，加强预警，重点保护基础信息网络和重要信息系统，从预防、监控、应急处理、应急保障和打击犯罪等环节，采取多种措施，共同构筑网络与信息安全保障体系。

2.快速反应。在网络与信息安全突发公共事件发生时，按照快速反应机制，及时获取充分而准确的信息，迅速处置，最大程度地减少危害和影响。

3.以人为本。把保障公共利益以及公民、法人和其他组织的合法权益的安全作为首要任务，及时采取措施，最大限度地避免

公民财产遭受损失。

4.分级负责。按照“谁主管谁负责、谁使用谁负责”以及“条块结合”的原则，建立和完善安全责任制及联动工作机制。根据部门职能，各司其职，加强协调与配合，形成合力，共同履行应急处置工作的管理职责。

（四）编制依据

根据《中华人民共和国突发事件应对法》和相关规定，制定本预案。

## 二、组织机构及职责

（一） 组织机构

成立突发网络与信息安全事件应急小组（以下简称网络与信息安全事件应急小组）。

组　长：任芳芳

副组长：刘玉华

成　员：王　志 马瑰芳 黄俊卿 姚沛元 房海波 宋雅南

（二） 网络与信息安全事件应急小组职责

1.负责编制、修订所辖范围内突发网络与信息安全事件应急预案。

2.通过本系统局域网络中心及国内外安全网络信息组织交流等手段获取安全预警信息，周期性或即时性地向局域网和用户网络管理部门发布；对异常流量来源进行监控，并妥善处理各种异常情况。

3.及时组织专业技术人员对所辖范围内突发网络与信息安全

事件进行应急处置；负责调查和处置突发网络与信息安全事件，及时上报并按照相关规定作好善后工作。

4.负责组建信息网络安全应急救援队伍并组织培训和演练。

**三、预防及预警机制**

突发网络与信息安全事件安全预防措施包括分析安全风险，准备应急处置措施，建立网络和信息系统的监测体系，控制有害信息的传播，预先制定信息安全重大事件的通报机制。

**（一）突发网络与信息安全事件分类**

网络与信息安全事件分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障和灾害性事件等。

**（二）突发网络与信息安全事件分级**

根据安全事件对业务造成的影响程度，安全级别从高到低为分级如下:

1.一级/紧急

安全事件造成业务中断或间断时间在30分钟以上，或者影响的范围涉及两个或两个以上业务系统，或者业务系统数据损坏、丢失，并且无法恢复，或者重要数据泄露，或者业务系统或网络被破坏或损坏，并且预计在30分钟内无法恢复。

2.二级/告警

安全事件造成业务中断或间断时间在15-30分钟，或者业务系统数据部分损坏、丢失，可以通过备份进行恢复。

3.三级/预警

安全事件造成业务中断或间断，中断时间1-15分钟，并且未

造成业务系统数据损坏、丢失。

4.四级/一般

安全事件未造成业务中断，或中断时间少于1分钟，并且未造成业务系统数据损坏、丢失。

（三）应急准备

单位信息系统管理员明确职责和管理范围，根据实际情况，安排应急值班，确保到岗到人，联络畅通，处理及时准确。

（四）具体措施

1.有害程序事件：分为计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件。

应对措施：一安装杀毒软件，对所运行的服务器实行统一管理、实时监测，及时修补系统漏洞、查杀木马程序、杜绝安全隐患的存在。二是建立统一的应用整体安全防御体系，实时扫描WEB系统的网页，查找网页挂马和非法程序，清除网页木马和非法程序，提高系统本身的安全性和可用性，保障应用系统安全运行。

2.网络攻击事件：分为拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件。

应对措施：建设网站应用系统主动防御平台，应对各种应用威胁，提高系统的抗攻击能力。

3.信息破坏事件：分为信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件、和其他信息破坏事件。

应对措施：通过建设应用系统主动防御平台，保障应用数据的访问、传输过程的安全，对访问者进行认证、授权、审计，最大限度的消除安全隐患。实现事前主动防御、智能分析应用缺陷、屏蔽恶意请求；事中智能响应，快速定位，阻止风险扩散，消除“安全事故”于萌芽之中；事后行为审计，深度挖掘访问行为、分析攻击数据，为评估安全状况提供详尽报表。

4.信息内容安全事件：是指网络传播法律、法规禁止的信息，阻止非法串联、煽动集会游行或者炒作敏感问题并危害国家安全、社会稳定和公众利益的事件。

应对措施：一是要建立严格的信息上网发布审计制度，门户网站发布信息必须有领导签字。二通过应用系统主动防御平台建立完善的信息上网审计，阻止不合法信息上网。

5.设备设施故障：分为软件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障。

应对措施：一是应用系统采用多台服务器集群部署，某台服务器出现故障不影响系统的正常运行。二是网络可采用多线路，多运营商不同路由接入，确保线路冗余，网络畅通。三是关键业务应用及数据采用多台存储实时同步备份、确保应用数据零丢失，应用系统安全、稳定运行。

## 四、应急预案

### （一）通信网络故障应急预案

1.发生通信线路中断、路由故障、流量异常、域名系统故障后，操作员应及时通知本单位信息系统管理员，经初步判断后及

时上报网络与信息安全事件应急小组。

2.系统管理员接报告后，应及时查清通信网络故障位置，隔离故障区域，并通知相关通信网络运营商查清原因；同时及时组织相关技术人员检测故障区域，逐步恢复故障区与服务器的网络联接，恢复通信网络，保证正常运转。

3.事态或后果严重的，网络与信息安全事件应急小组应及时报告科技信息处和相关业务部门。

4. 应急处置结束后，系统管理员和事发单位应将故障分析报告，在调查结束后一日内书面报告网络与信息安全事件应急小组。

（二）不良信息和网络病毒事件应急预案

1.发现不良信息或网络病毒时，信息系统管理员应立即断开网线，终止不良信息或网络病毒传播，并报告网络与信息安全事件应急小组。

2.系统管理员应采取隔离网络等措施，及时杀毒或清除不良信息，并追查不良信息来源。

3.处置结束后，系统管理员和事发部门应将事发经过、造成影响、处置结果在调查工作结束后一日内书面报告网络与信息安全事件应急小组。

（三）服务器软件系统故障应急预案

1.发生服务器软件系统故障后，系统管理员应立即组织启动备份服务器系统，由备份服务器接管业务应用，并及时报告网络与信息安全事件应急小组和科技信息处；同时安排将故障服务器脱离网络，保存系统状态不变，取出系统镜像备份磁盘，保持原

始数据。

2.系统管理员应在确认安全的情况下，重新启动故障服务器系统；重启系统成功，则检查数据丢失情况，利用备份数据恢复；若重启失败，立即联系相关厂商和上级单位，请求技术支援，作好技术处理。

3.事态或后果严重的，网络与信息安全事件应急小组及时报告信息中心。

4.处置结束后，系统管理员应将事发经过、处置结果等在调查工作结束后一日内报告网络与信息安全事件应急小组。

（四）黑客攻击事件应急预案

1.当发现网络被非法入侵、网页内容被篡改，应用服务器上的数据被非法拷贝、修改、删除，或通过入侵检测系统发现有黑客正在进行攻击时，使用者或管理者应断开网络，并立即报告网络与信息安全事件应急小组。

2.接报告后，网络与信息安全事件应急小组应立即指令系统管理员核实情况，关闭服务器或系统，封锁或删除被攻破的登陆帐号，阻断可疑用户进入网络的通道。

3.系统管理员应及时清理系统，恢复数据、程序，恢复系统和网络正常；情况严重的，应上报科技信息处，并请求支援。

4.处置结束后，系统管理员应将事发经过、处置结果等在调查工作结束后一日内报告网络与信息安全事件应急小组。

（五）核心设备硬件故障应急预案

1.发生核心设备硬件故障后，系统管理员应及时报告网络与

信息安全事件应急小组，并组织查找、确定故障设备及故障原因，进行先期处置。

2.若故障设备在短时间内无法修复，系统管理员应启动备份设备，保持系统正常运行；将故障设备脱离网络，进行故障排除工作。

3.系统管理员应在故障排除后，在网络空闲时期，替换备用设备；若故障仍然存在，立即联系相关厂商， 认真填写设备故障报告单备查。

4.事态或后果严重的，及时报告科技信息处。

（六）业务数据损坏应急预案

1.发生业务数据损坏时，系统管理员应及时报告网络与信息安全事件应急小组，检查、备份业务系统当前数据。

2.系统管理员负责调用备份服务器备份数据，若备份数据损坏，调用异地备份数据。

3.业务数据损坏事件超过 2 小时后，系统管理员应及时报告网络与信息安全事件应急小组，及时通知业务部门以手工方式开展业务。

4.系统管理员应待业务数据系统恢复后，检查历史数据和当前数据的差别，由相关系统业务员补录数据；重新备份数据，并写出故障分析报告，在调查工作结束后一日内报告网络与信息安全事件应急小组。

## 五、应急保障

（一）通信保障

系统管理员负责收集、建立突发网络与信息安全事件应急处置工作小组内部及其他相关部门的应急联络信息。网络与信息安全事件应急小组全体人员保证全天 24 小时通讯畅通。

（二）装备保障

系统管理员负责建立并保持电力、空调、机房等网络安全运行基本环境，预留一定数量的信息网络硬件和软件设备，指定专人保管和维护。

（三）数据保障

重要信息系统均建立备份系统，保证重要数据在受到破坏后可紧急恢复。

（四）队伍保障

建立符合要求的网络与信息安全保障技术支持力量，对网络接入单位的网络与信息安全保障工作人员提供技术支持和培训服务。

## 六、监督管理

（一）宣传教育和培训

将突发网络与信息安全事件的应急管理、工作流程等列为培训内容，增强应急处置能力。加强对突发网络与信息安全事件的技术准备培训，提高技术人员的防范意识及技能。网络与信息安全事件应急领导小组每年至少开展一次全市系统范围内的信息网络安全教育，提高信息安全防范意识和能力。

（二）预案演练

网络与信息安全事件应急小组每年至少安排一次演练，建立

应急预案定期演练制度。通过演练，发现和解决应急工作体系和工作机制存在的问题，不断完善应急预案，提高应急处置能力。

（三）责任与奖惩

网络与信息安全事件应急小组不定期组织对各项制度、计划、方案、人员及物资等进行检查，对在突发网络与信息安全事件应急处置中做出突出贡献的集体和个人，提出表彰奖励建议；对玩忽职守，造成不良影响或严重后果的，依法依规提出处理意见，追究其责任。

**七、附则**

结合信息网络快速发展和经济社会发展状况，配合相关法律法规的制定、修改和完善，适时修订本预案。本预案由开封市医疗保障局制定并负责解释。本预案发布之日起实施。

开封市医疗保障局办公室　　2020年10月19日印发