辖区妇幼健康信息安全应急预案

文件类别	全院文件-保健管理			文件编号	H-S-YA-001
制定部门	社会保健科	发布部门	质量管理科	生效日期	2020 年 8 月 10 日
版本/修订	B / 0	文件总页码	6	修订日期	年 月 日

1 目的

建立健全妇幼健康信息网络安全工作应急工作机制，提高应对网络与信息安全事件能力，预防和减少与信息安全事件造成的危害，维护妇幼健康信息系统安全和数据安全的稳定运行。

2 范围

辖区妇幼健康机构。

3 定义：无。

4 权责

4.1 本预案是由社会保健科负责制定、修订和解释；

4.2 各级妇幼健康机构负责实施和建议。

5 政策

5.1 组织机构

5.1.1 应急领导小组

a. 成员构成：由医院院长担任组长、分管辖区妇幼健康工作院领导任副组长、三大部负责人、社保科负责人、信息科负责人、辖区妇幼保荐机构分管领导组成。

b. 职责

a) 组织、指导和督促重大安全事件的应急响应工作；

b) 现场指挥重大安全事件应急响应；

c) 审定、批准应急方案的启用；

d) 组织协调各部门的应急合作、资源调配等工作；

e) 审定重大安全事件处理和分析报告。

5.1.2 技术保障组

a. 成员构成：由信息科人员技术人员构成。

b. 职责

a) 及时向应急领导小组上报发现的问题；

b) 提出初步的应急事件建议；

c) 对应急事件开始相应的处理，防止事件扩大；

d)运维人员全程参与应急事件处置。

5.2 基本原则

5.2.1 统一领导，分级负责。按照“谁主管谁负责”的原则，建立和完善责任制度、协调管理机制和联动工作机制。

5.2.2 快速反应，积极应对。一旦发生网络和信息系统环境和业务系统突发事件，应迅速启动应急处置预案，明确职责，层层落实，采取有力措施积极应对，及时控制处理，防止产生连带风险。

5.2.3 加强沟通，有效传递。建立有效的信息传递机制，各辖区妇幼健康机构协作，确保信息畅通；

5.2.4 保密数据，严格管理。在应急预案正式启动期间，各级要做好数据资料的保密保管工作，明确数据资料保管责任人，资料接触人员要严格保密，决不随意向任何人泄漏，应急期间结束后，统一存档。

5.2.5 严格自律，防范风险。突发事件应急处置期间，各辖区妇幼健康信息部门应加强宣传教育和检查监督，引导员工严格自律，遵守内控制度和业务操作要求，向社会作正面解释、宣传，不得散播影响单位形象和社会稳定的言论，严密防范内、外部潜在风险。

5.2.6 准确判断，及时响应。安全事件发生后，及时确定事件分类、级别，启动对应的响应措施。

5.3 安全事件分级

5.3.1 依据《信息安全事件分类分级指南》(GBZ 20986-2007)技术文件要求，将信息安全事件划分为 4 个级别：一般事件(Ⅳ级)、较大事件(Ⅲ级)、重大事件(Ⅱ级)、特别重大事件(Ⅰ级)

a.一般事件（Ⅳ级）：一般事件是指不满足以上条件的网络和信息安全事件，包括以下情况

a)会使特别重要网络信息系统遭受较小的系统损失、或使重要网络和信息系统遭受较大的系统损失，一般信息系统遭受严重或严重以下级别的系统损失；

b)产生一般的社会影响。

b.较大事件（Ⅲ级）：较大事件是指能够导致较严重影响或破坏的网络和信息安全事件，包括以下情况

a)会使特别重要网络和信息系统遭受较大的系统损失、或使重要网络和信息系统遭受严重的系统损失，一般网络和信息系统遭受特别严重的系统损失；

b)产生一般的社会影响。

c.重大事件（II级）：重大事件是指能够导致严重影响或破坏的网络和信息安全事件，包括以下情况

a)会使特别重要网络和信息系统遭受严重的系统损失、或使重要网络和信息系统遭受特别严重的系统损失；

b)产生重大的社会影响。

d.特别重大事件（I 级）：特别重大事件是指能够导致特别严重影响或破坏的网络和信息安全事件，包括以下情况

a)会使特别重要网络和信息系统遭受特别严重的系统损失；

b)产生特别重大的社会影响。

5.3.2 依据《信息安全事件分类分级指南》(GBZ 20986-2007)，结合自身实际情况，我院将安全事件分级如下

a.Ⅳ级：应用服务器双机中的一台设备故障或小范围网络瘫痪，不影响系统正常运行，只影响个别科室使用。

b.Ⅲ级：应用服务器设备故障或大范围网络瘫痪，影响部分系统病区或者门诊正常运行。

c.Ⅱ级：应用服务器设备故障或全部网络瘫痪，或应用系统出现严重错误，影响医院所有系统正常运行。

d. Ⅰ 级：应用服务器设备严重故障或全部网络瘫痪，或应用系统出现特别严重错误，长时间影响医院所有系统正常运行。

5.4 预防预警

5.4.1 信息监测及报告

建立运维监控系统，对于服务器、网络、数据进行实时监控。

5.4.2 严格数据保密管理

在应急预案正式启动期间，各级要做好数据资料的保密保管工作，明确数据资料保管责任人，资料接触人员要严格保密，决不随意向任何人泄漏，应急期间结束后，统一存档。

5．5 应急响应和处置

5.5.1 应急响应

a.IV 级响应时，遵循以下步骤

a)此类事件严重程度一般，可不向应急领导小组汇报，由信息科负责人直接将任务分配给技术保障小组；

b)技术保障小组快速定位引起系统故障的原因，进行故障排除；

c) 故障排除恢复业务后，技术保障小组分析和总结事件发生的原因，完善整改措施，向信息科负责人汇报，信息科负责人根据情况决定是否向应急领导小组进行汇报。

b. III 级响应时，遵循以下步骤

a) 事件发生后，信息科负责人将任务分配给技术保障小组；

b) 技术保障小组定位故障原因，预估恢复业务事件，如果在 30 分钟内可以解决问题，则可暂不向应急领导小组组长和副组长汇报，若不能在 30 分钟内解决则应向应急领导小组副组长汇报，由副组长进行应急指挥；

c) 根据应急领导小组副组长分派的任务，综合协调小组负责通知相关业务科室启动应急预案，同时联系相关部门进行综合保障；

d) 技术组进行故障查找和排除，进行数据修复和系统恢复的工作，对于不能处理的问题及时联系维保厂商和专家进行远程和现场支持。

c. II 级以上响应时，除以上流程外，还应逐级上报主管部门。

5.5.2 技术保障组应急处置

a. 数据恢复方面

a) 在数据库遭破坏或损毁时，及时启动灾难性数据恢复机制，采用备份数据进行恢复，若建立了数据容灾系统，应迅即启用容灾备份系统支持正常业务开展；

b) 在硬件损坏修复时，遵守数据安全、完整第一原则，首先在保证存储介质不受损伤的情况下进行维修。

b. 网络故障处理

如属线路故障，应通知相关人员检修维护或重新安装线路。

c. 硬件设备故障

若属于机器硬件设备故障，应立即用备件替换受损部件。如属不能自行恢复的，

立即与设备提供商联系，请求维护人员前来维修。

d. 恢复工作的告知

协调组及时告知相关科室系统恢复的进程，以便相关部门及时调整相应工作流程。如果设备和信息系统修复所需时间较长，应通过电话、医院网站、新闻媒体等方式做好宣传解释工作。

5.5.3 相关业务科室手工业务应急处置：突发事件发生后，在保证业务处理的连续性和数据完整性的原则下，各相关科室和部门应紧密配合，负责人到现场及时处理特殊事件，先采用手工处理相关业务，切实保障业务不

间断运行，待系统恢复正常后，及时将业务流程切换到正常状态。

5.6 应急响应和处置

5.6.1 事后总结：应急结束后，由应急响应助理、日常运维小组、技术保障小组分析和总结事件发生的原因；评估系统的损害程度；总结经验教训；提出改进办法；完善整改措施；上报处理结果。

5.6.2 善后处置：在应急处置工作结束后迅速采取措施，抓紧组织抢修受损的基础设施，减少损失，尽快恢复正常工作。统计各种数据，查明原因，对事件造成的损失和影响以及恢复重建能力进行分析评估，认真制定恢复重建计划，迅速组织实施，并将善后处置的有关情况报应应急领导小组组长或副组长。

5.6.3 调查报告和经验教训总结及改进建议

a. 在突发网络和信息安全事件应急处置结束后，技术保障小组根据需要对起因、性质、影响、财产损失、采取的处置措施等情况组织调查并形成报告，组织力量进行全面审核评估，认真总结经验与教训，防止同类事件的发生，于调查工作结束后3日内，提交书面报告。

b. 书面报告的内容包括：事发部门的详细名称、发生的准确时间及地点、初步原因、直接经济损失及造成社会影响、详细处置过程、采取的处置措施、控制程度、参与处置的人员及经验和教训、预防以后此类网络和安全事件发生的措施、对预案的修改建议、报告时间。

6 工作流程：无。

7 标准/依据

7.1 法律法规

7.1.1 《中华人民共和国网络安全法》，自2017年6月1日起施行。

7.1.2 《中华人民共和国计算机信息系统安全保护条例》，自2012年2月7日发布。

7.2 有关标准

7.2.1《信息安全技术-网络安全等级保护基本要求》，GB/T 22239-2019，自2019年12月1日起施行。

8 表单附件：无。

9 文件修订记录

修订日期	修订后版本	更改的内容描述

10 审核批准

部　　门		审核/批准签字	签署日期
主　办	社会保健科	部门负责人：林晓杰	2020年8月10日
协　办	孕产保健部	部门负责人：高丽丽	2020年8月10日
	妇女保健部	部门负责人：宋维花	2020年8月10日
	儿童保健部	部门负责人：陈　婧	2020年8月10日
院领导批准		分管领导：黄玉强	2020年8月10日