网络安全现状及重点工作安排

委规划发展与信息化处　李磊

2019年4月25日

目录

CONTENTS

目录
CONTENTS

2018年网络安全检查情况

2018年对63家卫生健康机构进行了现场检查，首次检查17市全民健康信息平台，对上年度网络安全检查排名靠后的46家医疗机构“回头看”

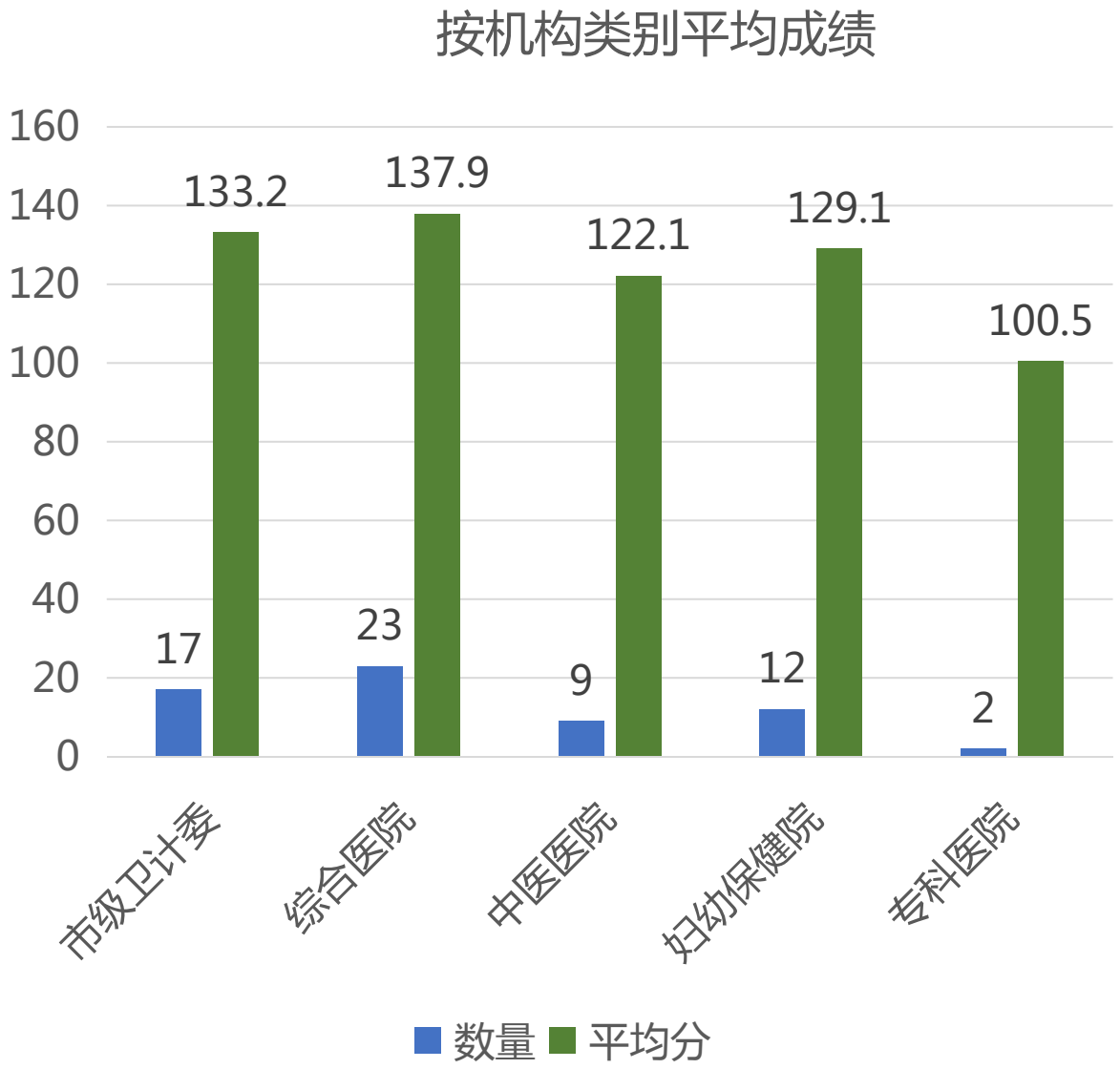
- 17市全民健康信息平台
- 综合医院21家
- 中医医院11家
- 妇幼保健医院12家
- 专科医疗机构2家

评价指标总分200分，被检查的63家单位平均分为131.4分。

主要结果分析

从机构类别来看

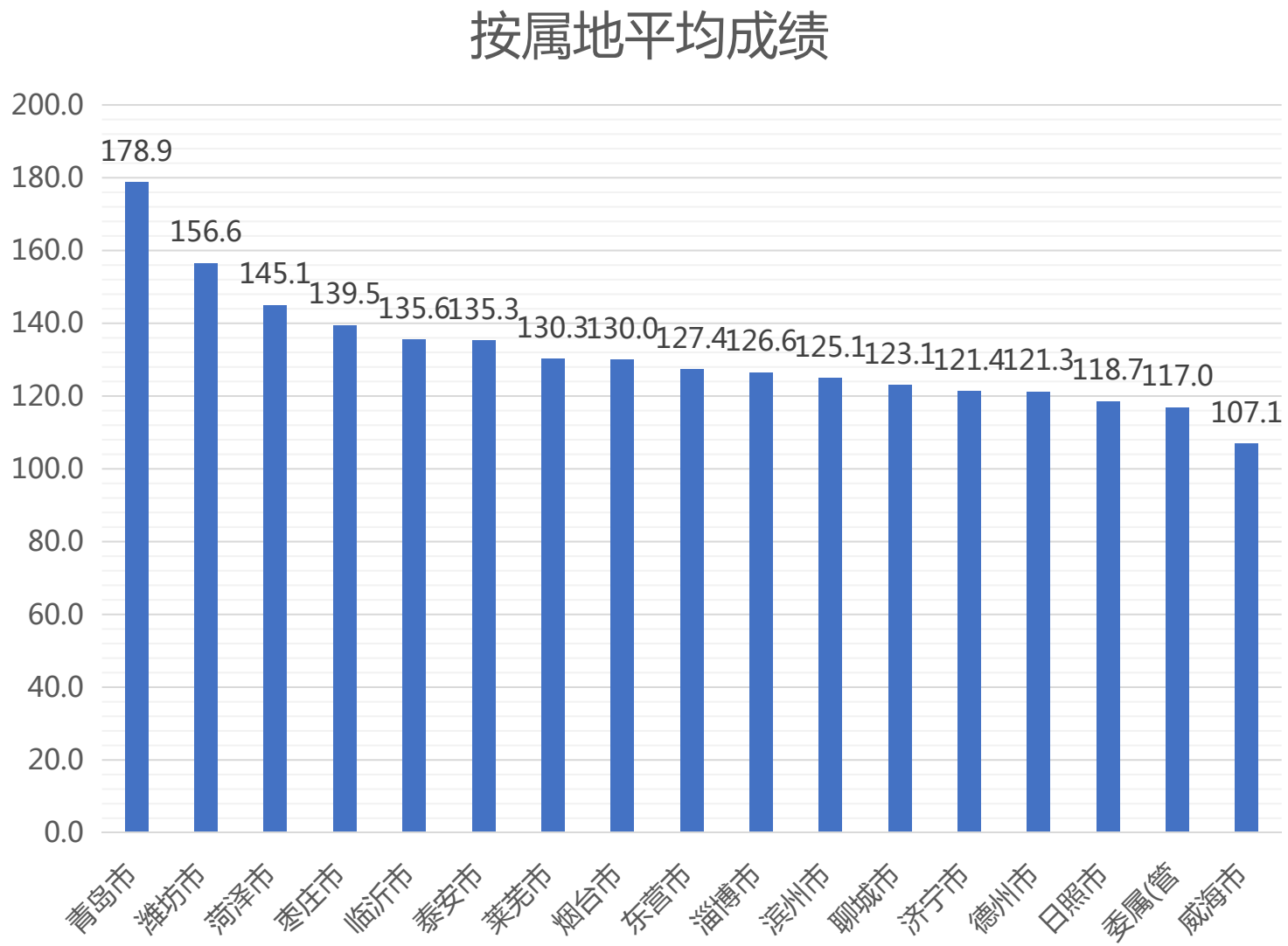
- 综合医院平均成绩为137.9分
- 市级平台平均成绩为133.2分
- 妇幼保健院平均成绩为129.1分
- 中医医院平均成绩为122.1分
- 其他机构2家平均成绩为100.5分。



主要结果分析

从属地来看

- 青岛市最好，平均178.9分
- 潍坊市、菏泽市位居2、3位
- 日照市、威海市排名倒数
- 尤其是检查的委属（管）单位平均成绩仍然排名倒数。



主要结果分析

从综合评价等级来看

按照管理体系建设、自查工作、安全专项、技术防护四个维度，把行业单位网络安全工作水平划为5个级别：

市全民健康信息平台：

- L5级　0家
- L4级　2家：济南、青岛
- L3级　3家：威海、滨州、烟台
- L2级　8家：潍坊、淄博、枣庄、东营、德州、菏泽、莱芜、泰安
- L1级　4家：日照、聊城、济宁、临沂

主要结果分析

从综合评价等级来看

医疗卫生单位：

- L5级 0家
- L4级 8家
- L3级 13家
- L2级 26家
- L1级 16家

序号	单位名称	所属	级别
1	青岛市市立医院	青岛市	L4
2	青岛市妇女儿童医保中心	青岛市	L4
3	聊城市第二人民医院	聊城市	L4
4	潍坊市人民医院	潍坊市	L4
5	山东省立第三医院	委属(管)	L4
6	菏泽市中医医院	菏泽市	L4
7	菏泽市单县中心医院	菏泽市	L3
8	潍坊医学院附属医院	潍坊市	L3
9	滕州市中心人民医院	枣庄市	L3
10	诸城市人民医院	潍坊市	L3
11	胜利油田中心医院	东营市	L3
12	东营市人民医院	东营市	L3
13	枣庄市妇幼保健院	枣庄市	L3
14	德州市妇幼保健所	德州市	L3
15	莱芜市妇幼保健院	莱芜市	L3
16	临沂市妇女儿童医院	临沂市	L3

网络安全检查主要成绩

网络安全管理体系建设

网络安全监管责任和主体责任落实力度有所提高，63家单位全部建立了比较完善的网络安全领导管理机构，人员岗位和人员教育培训比较完善，应急预案及应急演练持续改进。

01

网络安全专职队伍建设

有47家（约占74%）单位配备了专（兼）职网络安全管理员，较去年同比高出12%，有20家（约占32%）单位网络安全管理员拥有国家认可的网络安全管理人员资质，较去年同比高出10%。

02

网络安全资金保障加大

17市卫生计生委三年来信息化投资总额约为2.44亿元，其中网络安全建设专项资金投入总额约为0.3亿元，约占信息化投资总额的12%；46家医院三年来信息化投资总额约为10亿元，其中网络安全建设专项资金投入总额约为1.69亿元，约占信息化投资总额的16.9%，安全经费占信息化费用比例≥10%的单位数量超过50家。

03

网络安全合规性增强

各市卫生健康委中有12家完成网络安全等级测评工作，占全部单位的70%；46家医院中有34家单位完成了网络安全等级保护评测工作，占全部单位的74%。

04

网络安全取得突破性进展

在本次检查中青岛市市立医院、青岛市妇女儿童医院、聊城市第二人民医院、潍坊市人民医院、省立第三医院、菏泽市中医医院（按成绩排序）在去年检查反馈基础上，网络安全整改工作高度重视、扎实推进、实效明显。

05

存在的主要问题

网络安全责任制未全面落实到位

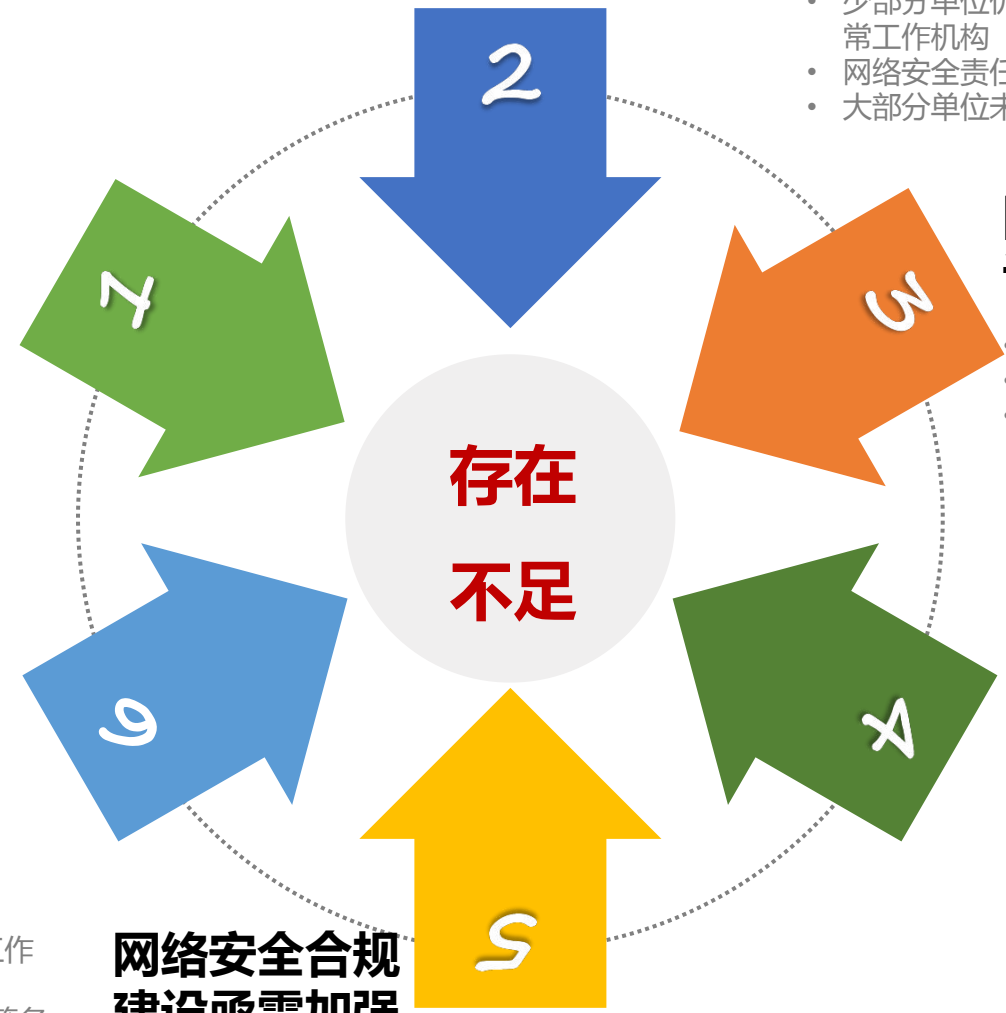
- 不重视、不重视、不重视
- 大部分单位对网络风险认识仍然不够充分
- 认为自身内部业务系统与外界交互少，没有必要做更高级别安全防护的必要性，低估了网络风险的破坏性和内部风险的可能性
- 认为网络安全设备投入比较多，已经可以确保网络安全，而日常管理和安全运维工作缺位，忽视了不断产生的新风险

新技术新业态网络安全亟须进一步加强

- 绝大部分单位上线的掌上医院、互联网医院、预约挂号系统等新技术应用项目未开展上线前的系统软件测评和网络风险评估与评测
- 上云单位、云服务商（含政务中心）、系统研发单位、系统维护单位在云服务网络安全工作上责权分工不明确，业务边界不清晰
- 部分机构部署的商保直赔系统在知情授权、数据授权、个人隐私保护和数据安全等方面存在严重管理缺位、技防缺失
- 部分互联网医院（含掌上医院、预约挂号等）在网络部署、数据安全、个人隐私保护等方面管理缺位、技防缺失。

- 近1/4的单位未能开展网络安全等级保护工作
- 80%以上的单位未开展国产密码应用工作
- 80%以上的单位电子病历系统未使用电子签名签章技术。

网络安全合规建设亟需加强



网络安全管理体系建设亟待进一步完善

- 缺乏网络安全整体规划和顶层设计
- 少部分单位仍然未建立网络安全领导机构和日常工作机构
- 网络安全责任制只说不做搞形式
- 大部分单位未建立信息资产台账

网络安全专业技术人才队伍建设有待于进一步加强

- 部分单位仍然没有专职的网络安全管理员
- 各单位网络安全技术继续教育严重不足
- 在自身技术能力不足的情况下，未能引进专业人才或者购买第三方网络安全专业服务来加强自身技术防护能力。

网络安全资金保障没有形成长效机制

- 近年来大部分单位资金投入虽有明显增加，但仍未形成制度化的网络安全资金保障机制
- 由于历史欠账较多，网络安全资金投入总额仍显不足。
- 大多数单位在资金使用上普遍存在着“重技术、轻管理，重形式、轻过程，重建设、轻运维，重执行、轻监督”的情况。

目录
CONTENTS

网络安全制度清单

国家及部委文件

01 中华人民共和国网络安全法

02 关键信息基础设施安全保护条例

03 党委(党组)网络安全工作责任制实施办法

04 网络安全等级保护制度2.0（预计4月底发布）

05 个人信息安全规范GBT35273-2017

06 健康医疗信息安全指南

07 数据出境安全评估指南

网络安全制度清单

国家卫生健康委文件

01 “十三五”全民健康网络与信息安全规划

02 关于进一步加强全民健康网络与信息安全工作的通知

03 国家卫生计生委网络安全应急预案

04 国家健康医疗大数据标准、安全和服务管理办法（试行）

05 关于落实卫生健康行业网络信息与数据安全责任的通知

网络安全制度清单

省卫生健康委文件

01 关于进一步加强全省卫生计生行业商用密码应用工作的通知（鲁卫规划字〔2017〕9号）

02 关于进一步加强全省卫生计生行业网络安全等级保护工作的通知（鲁卫规划字[2017]10号）

03 关于成立山东省卫生和计划生育委员会网络安全技术专家委员会的通知([2017]11号)

04 关于印发山东省卫生计生行业网络安全工作评价指标(试行)的通知（鲁卫规划字〔2017〕14 号)

05 关于印发排查整改重要业务数据和公民个人信息泄漏安全隐患专项工作方案的通知

网络安全制度清单

近期即将出台文件

01 关于进一步加强落实山东省卫生健康行业单位网络安全责任制的通知

02 山东省卫生健康行业网络安全工作责任制目标分解指标（试行）

03 山东省卫生健康行业云计算服务网络安全管理规范（试行）

04 山东省卫生健康行业云服务能力评价指标（试行）

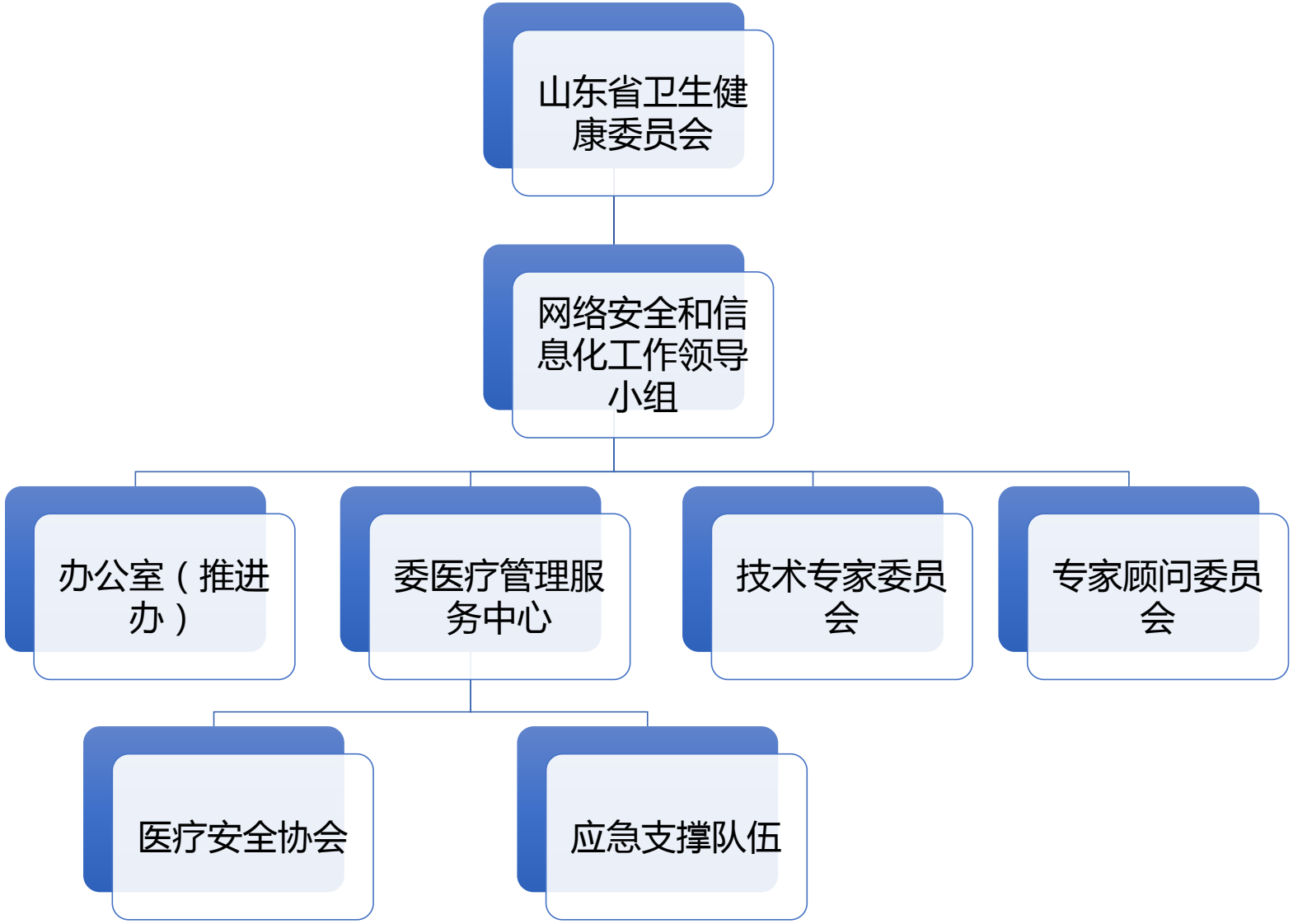
05 山东省互联网医院网络安全管理规范（试行）

06 山东省医院网络安全基线标准规范（试行）

07 山东省健康云计算服务网络安全合作框架参考协议

目录
CONTENTS

网络安全组织架构


山东省卫生健康委员会
网络安全和信息化工作领导小组
办公室（推进办）
委医疗管理服务中心
技术专家委员会
专家顾问委员会
医疗安全协会
应急支撑队伍

网络安全工作思路

依据《网络安全法》等法规，加强网络安全宣传，按照“自主保护、重点防护、同步规划建设、动态调整”的原则，不断完善全省卫生健康行业网络安全制度和标准规范，以网络安全等级保护、关键信息技术设施防护和国产密码应用为重点，推进行业网络安全管理体系建设、网络可信体系建设和人才队伍建设，以网络安全检查为抓手，“以查促建，以查促改”，不断提高行业网络安全监测能力、防护能力和处置能力，保障各级医疗卫生机构安全可靠、持续平稳为群众提供医疗健康服务和健康医疗信息服务。

网络安全下步工作要求

党委(党组)

网络安全工作责任制实施办法

网络安全下步工作要求

HINSF Health Network Security Forum 2017 医疗网络安全论坛

一、落实网络安全工作责任制

中共中央办公厅 厅字【2017】32号
《党委（党组）网络安全责任制实施办法》

网络安全下步工作要求

HINSF Health Network Security Forum 2017 医疗网络安全论坛

一、落实网络安全工作责任制

重要系统瘫痪

党政机关门户网站、重要网络平台被攻击篡改，导致反动言论或者谣言等违法有害信息大面积扩散，没有及时报告和组织处理的，或者瘫痪6小时以上的；

信息泄露

发生国家秘密泄露、大面积个人信息泄露或者大面积国家基础数据泄露的；

关键信息基础设施被攻击

关键信息基础设施遭受网络攻击，没有及时处置导致大面积影响人民群众工作、生活，或者造成重大经济损失，或者造成严重不良社会影响的；

网络安全事件瞒报漏报&整改不及时

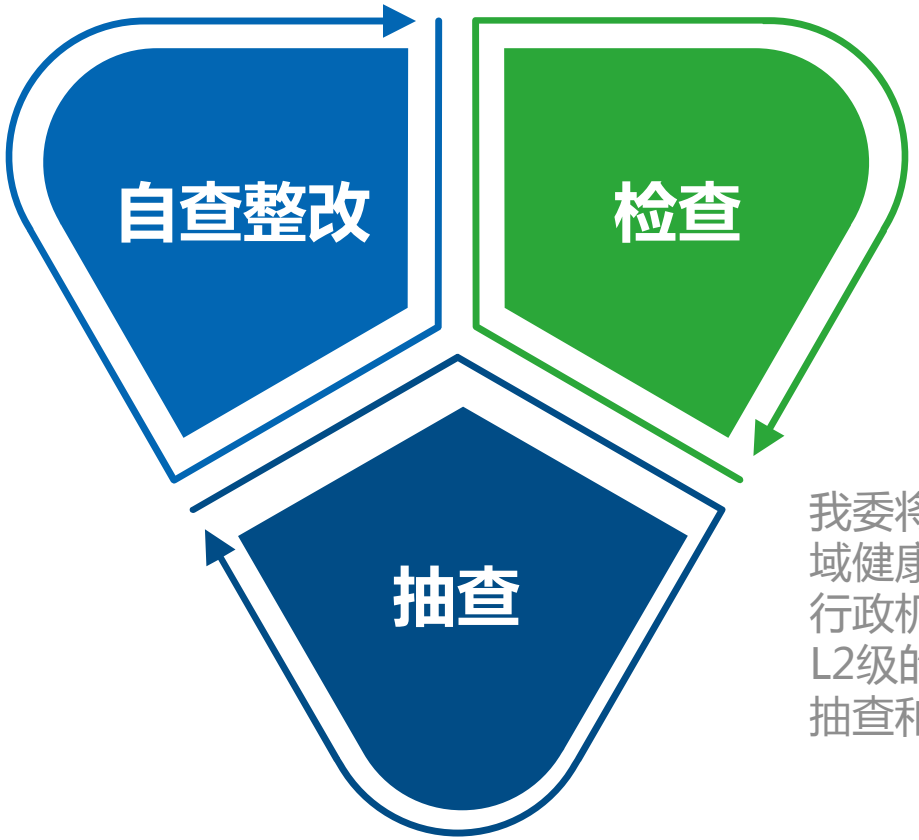
封锁、瞒报网络安全事件情况，拒不配合有关部门依法调查、处置工作，或者对有关部门通报的问题和风险隐患不及时整改造成严重后果的。

网络安全下步工作要求

HINSF Health Network Security Forum 2017 医疗网络安全论坛

二、继续开展网络安全自查整改、检查、抽查工作

2018年被查单位要逐一制定整改落实计划，其他单位要举一反三，针对共性问题认真开展安全风险评估和隐患排查，深入分析本单位主要风险和威胁，结合实际工作，建立问题台账，制定有针对性地工作措施并确保落实到位，确保2019年6月底之前完成整改加固工作。

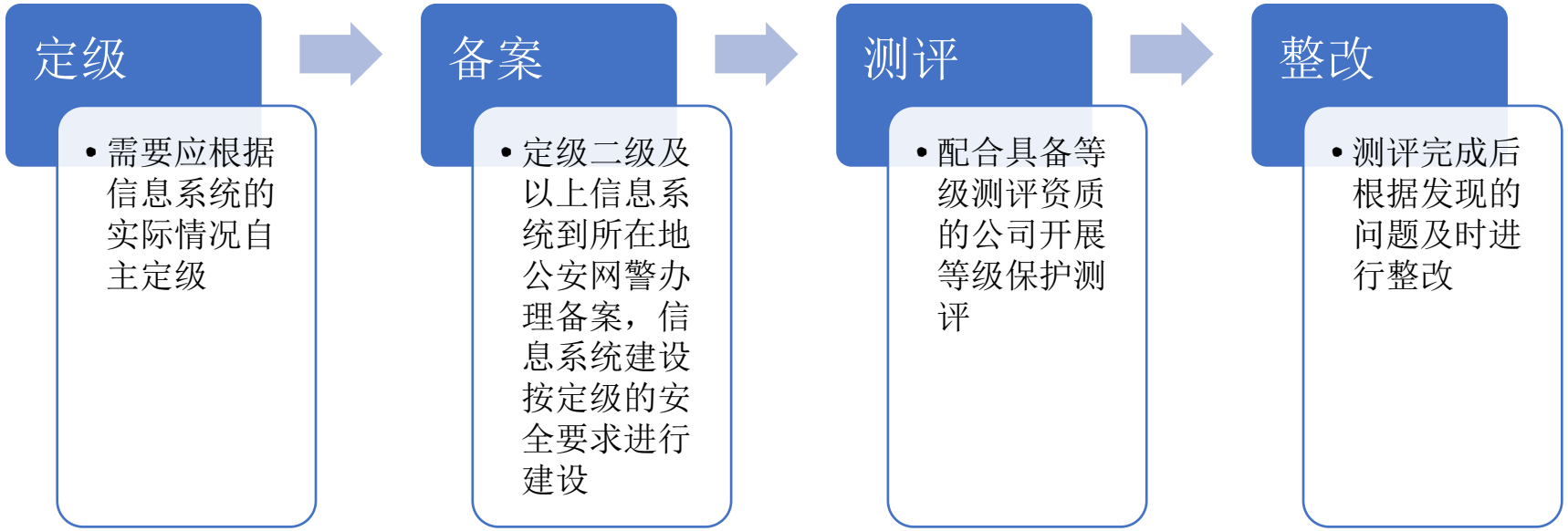


各市卫生健康委须于2019年8月底之前组织专家技术力量对在辖区单位组织一次网络安全检查，全面深入开展安全风险评估和隐患排查，对发现的问题及时通报，督促各单位及时完成整改工作。

我委将适时安排回头看，重点针对有区域健康信息平台的市（县）级卫生健康行政机构、二级以上医院、评级在L1、L2级的单位及分项排名靠后的单位进行抽查和再次督查。

网络安全下步工作要求

三、严格依法开展信息系统等级保护



等级保护2.0上线之后，按等保2.0要求进行重新测评。

各市、各单位须在2019年10月前完成重要网络系统的等级保护定级、评测和整改工作。

网络安全下步工作要求

四、加强单位重要数据和个人信息的保护

各单位梳理出业务系统的重要数据和个人敏感信息数据

按要求对单位重要数据和个人信息数据进行上报

目前信息基础设置数量较大并且统计不全，下一步各单位梳理出关健信息基础设施，分类保护重要不同的设施

按照关键信息基础设施安全保护条例、数据出境安全评估指南和个人信息安全规范对数据加强保护，筛检出重要、敏感的数据单独加密存放，个人信息也分类保护

山东省卫生健康委员会

鲁卫函〔2019〕124号

山东省卫生健康委员会
关于印发《全省卫生健康系统重要数据和公民个人信息泄漏安全隐患排查整改专项工作方案》的通知

各市卫生健康委，委属(管)各单位：

根据公安部、国家卫生健康委和省公安厅部署要求，我委确定在全省卫生健康系统开展重要数据和公民个人信息泄露安全隐患排查整改工作，研究制定了《全省卫生健康系统重要数据和公民个人信息泄漏安全隐患排查整改专项工作方案》。现将工作方案印发给你们，请各市各单位认真落实网络安全主体防护责任，切实加强对重要数据和公民个人信息的安全保护，并按方案要求做好各项工作，对发现的隐患及时整改，并按时上报数据。

山东省卫生健康委员会
2019年4月10日

（信息公开形式：依申请公开）

网络安全下步工作要求

五、加强互联网应用系统（网站）安全防护

互联网应用梳理

各单位梳理出目前正在使用的互联网应用系统，特别是网站。

下线或集约化建设

对互联网应用系统进行检测、整改，有严重问题的下线整改，也可依据系统的功能性来集约化建设，打造完善的互联网应用系统。

网站日常防护

对在日常管理中对互联网应用加强防护工作，合理使用网络安全设备如WAF、堡垒机、玄武盾等保护应用不被不法分子利用。

加强云服务管理

各单位应加强云服务的安全规范化管理，保证云服务中信息系统的安全。对提供云服务的供应商实施标准化评价，保证提供的云服务具备较高的安全性。

网络安全下步工作要求

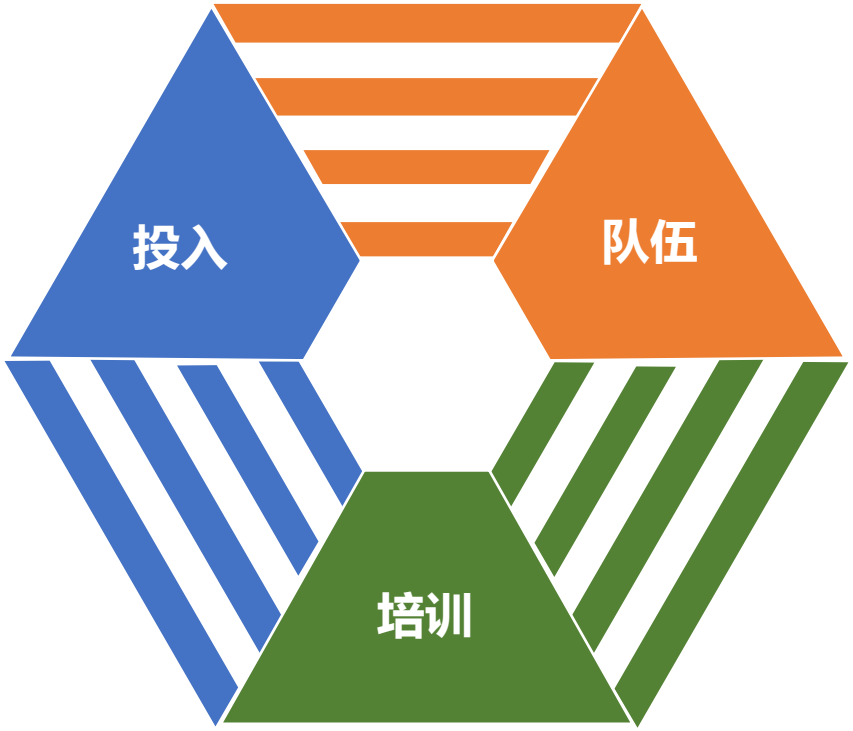
六、及时完成IT信息资产登记

- 各市、各单位及时登录“省卫生健康行业网络安全综合监管服务系统”报送信息资产、网络安全等级保护、国产密码应用、关键信息基础设施、网络安全问题台账、整改计划和网络安全事件等信息，定时接收网站和移动APP（微信公众号）安全扫描报告、网络安全检查评估报告等，逐步实现网络安全风险动态评估长效机制。
- 2019年6月之前，各市卫生计生委和全省二级（含）以上卫生健康单位须通过省卫生健康行业网络安全综合监管服务系统完成相关数据上报。

网络安全下步工作要求

七、完善长效机制建设

各单位信息化总投入应占单位全年总收入（财政总预算）的1-5%，网络安全总投入应不低于全年信息化总投入的10%；要进一步加大网络安全规划咨询和运维管理等重点领域的资金投入。



各单位须配置不少于1名具备国家认可资质的网络安全管理员（网络安全等级保护联络员），负责单位网络安全具体工作；单位内部各部门须在至少配置1名信息化联络员，负责本部门信息化和网络安全具体工作。

各单位从安全政策、安全意识、管理防范、技术防范等方面加大培训力度，提高专业人员的业务能力和水平。各市、各单位每年至少组织一次全员网络安全意识教育，至少要组织一次网络安全教育宣传活动（配合网络安全宣传周）。

网络安全下步工作要求

八、举办全省卫生健康系统网络安全和信息化技能竞赛

- 全省卫生健康系统网络安全和信息化技能竞赛活动由省卫生健康委与省总工会联合举办。省卫生健康委规划发展与信息化处、省医务工会、省卫生健康委医疗管理服务中心具体承办，省网络安全协会医疗分会协办。
- 全省卫生健康系统网络安全与信息化技能竞赛活动形式包括岗位练兵和技能竞赛，技能竞赛分为县级竞赛、市级竞赛和省级复赛、决赛4个阶段。
- 特等奖获得者将由省医务工会工作委员会向省总工会申报“山东省富民兴鲁劳动奖章”。

谢谢聆听