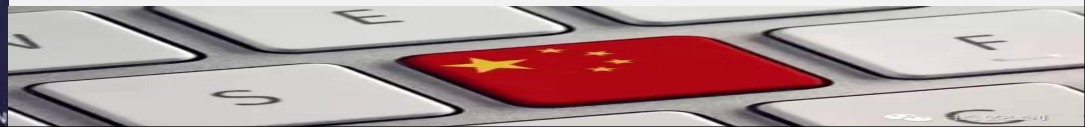
HNSF
Health Network Security Forum 2017
医疗网络安全论坛

贯彻落实网络安全法
做好医疗机构等级保护

北京市卫生计生委信息中心

郑攀

2019年4月25日



目录
CONTENT

出席委员	赞成	反对	弃权
155	154	0	1

中华人民共和国主席令

第 五十三号

《中华人民共和国网络安全法》已由中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议于2016年11月7日通过，现予公布，自2017年6月1日起施行。

中华人民共和国主席　习近平

2016年11月7日

中华人民共和国网络安全法

（2016 年 11 月 7 日第十二届全国人民代表大会常务委员会第二十四次会议通过）

目　录

79条

关注大事儿-《网络安全法》

- 首次宣誓了国家保卫网络空间主权的原则
- 进一步确立了等级保护制度的法律地位
- 明确了在等级保护的基础上，重点加强关键信息基础设施安全保护
- 进一步明确了网络运营者、网络产品和服务提供者的义务及个人信息保护规则
- 明确了网络安全国家审查，确立了关键信息基础设施重要数据跨境传输的规则

《网络安全法》相关条款

口 **第二十一条** 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

《网络安全法》相关条款

口 **第三十一条** 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制

《网络安全法》相关条款

口 **第三十八条** 关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。（等级测评

法律责任

口**第五十九条** 网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款；对直接负责的主管人员处五千元以上五万元以下罚款。关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款；对直接负责的主管人员处一万元以上十万元以下罚款。

当前的任务

- 全面实行信息安全等级保护制度 等保2.0

  定级、备案、整改、测评

- 在等级保护的基础上，重点保护关键信息基础设施

- 全面自查门户网站和核心业务系统安全

等级保护2.0定级要求解析

新增“定级流程”

包括基础信息网络、工业控制系统、云计算平台、物联网、其他信息系统、大数据等。

包括确定受侵害的客体、侵害对客体的侵害程度以及综合判定侵害程度。

定级对象的运营、使用单位应组织信息安全专家和业务专家，对初步定级结果的合理性进行评审，出具专家评审意见。

定级对象的运营、使用单位应将初步定级结果上报行业主管部门或上级主管部门进行审核。

定级对象的运营、使用单位应按照相关管理规定，将初步定级结果提交公安机关进行备案审查，审查不通过，其运营使用单位应组织重新定级；审查通过后最终确定定级对象的安全保护等级。

注：基于GA/T 1389—2017《网络安全等级保护定级指南》及GB/T 22240—2008《信息系统安全等级保护定级指南》内容对比分析。

等级保护2.0定级要求解析

定级对象

- **重新对定级对象进行调整，并进行相应的介绍。2.0定级对象分为基础信息网络、信息系统和其他信息系统，其中信息系统再细分为工业控制系统、物联网、大数据、移动互联以及云计算平台。**

1.0要求

信息系统

~~一个单位内运行的信息系统可能比较庞大，为了体现重要部分重点保护，有效控制信息安全建设成本，优化信息安全资源配置的等级保护原则，可将较大的信息系统划分为若干个较小的、可能具有不同安全保护等级的定级对象。~~

2.0要求

工业控制系统

工业控制系统主要由生产管理层、现场设备层、现场控制层和过程监控层构成，其中：生产管理层的定级对象确定原则见(其他信息系统)。设备层、现场控制层和过程监控层应作为一个整体对象定级，各层次要素不单独定级。

对于大型工业控制系统，可以根据系统功能、控制对象和生产厂商等因素划分为多个定级对象。

物联网

物联网应作为一个整体对象定级，主要包括感知层、网络传输层和处理应用层等要素。

采用移动互联技术的信息系统

采用移动互联技术的等级保护对象应作为一个整体对象定级，主要包括移动终端、移动应用、无线网络以及相关应用系统等。

大数据

应将具有统一安全责任单位的大数据作为一个整体对象定级， 或将其与责任主体相同的相关支撑平台统一定级。

云计算平台

在云计算环境中，应将云服务方侧的云计算平台单独作为定级对象定级， 云租户侧的等级保护对象也应作为单独的定级对象定级。

对于大型云计算平台，应将云计算基础设施和有关辅助服务系统划分为不同的定级对象。

基础信息网络

对于电信网、广播电视传输网、互联网等基础信息网络，应分别依据服务类型、服务地域和安全责任主体等因素将其划分为不同的定级对象。

跨省全国性业务专网可作为一个整体对象定级，也可以分区域划分为若干个定级对象。

其他信息系统

作为定级对象的其他信息系统应具有如下基本特征：

a) **具有确定的主要安全责任单位。**作为定级对象的信息系统应能够明确其主要安全责任单位；

b) **承载相对独立的业务应用。** 作为定级对象的信息系统应承载相对独立的业务应用， 完成不同业务目标或者支撑不同单位或不同部门职能的多个信息系统应划分为不同的定级对象；

c) **具有信息系统的基本要素。** 作为定级对象的信息系统应该是由相关的和配套的设备、 设施按照一定的应用目标和规则组合而成的多资源集合，单一设备（如服务器、终端、网络设备等）不单独定级。

注：基于GA/T 1389—2017《网络安全等级保护定级指南》及GB/T 22240—2008《信息系统安全等级保护定级指南》内容对比分析。

等级保护2.0标准体系

等保1.0 | 等保2.0

四、标准控制点与要求项的变化：新标准控制点并没有明显的增加，通过合并**整合后反而减少了**。

通用安全要求1.0	通用安全要求分类	控制点	
		二级	三级
技术要求	物理安全	10	10
	网络安全	6	7
	主机安全	6	7
	应用安全	7	9
	数据安全	3	3
管理要求	安全管理制度	3	3
	安全管理机构	5	5
	人员安全管理	5	5
	系统建设管理	9	11
	系统运维管理	12	13
合计		66	73

通用安全要求2.0	通用安全要求分类	控制项	
		二级	三级
技术要求	安全物理环境	10	10
	安全通信网络	3	3
	安全区域边界	6	6
	安全计算环境	10	11
	安全管理中心	2	4
管理要求	安全管理制度	4	4
	安全管理机构	5	5
	安全管理人员	4	4
	安全建设管理	10	10
	安全运维管理	14	14
合计		68	71

各级的控制点数量变化如上表所示。

通用安全要求1.0	通用安全要求分类	控制点	
		二级	三级
技术要求	物理安全	19	32
	网络安全	18	33
	主机安全	19	32
	应用安全	19	31
	数据安全	4	8
管理要求	安全管理制度	7	11
	安全管理机构	9	20
	人员安全管理	11	16
	系统建设管理	28	45
	系统运维管理	41	62
合计		175	290

通用安全要求2.0	通用安全要求分类	控制项	
		二级	三级
技术要求	安全物理环境	15	22
	安全通信网络	4	8
	安全区域边界	11	20
	安全计算环境	23	34
	安全管理中心	4	12
管理要求	安全管理制度	6	7
	安全管理机构	9	14
	安全管理人员	7	12
	安全建设管理	25	34
	安全运维管理	31	48
合计		135	211

控制项在合并的情况下也有所减少，详见上图。

点击添加相关标题文字

安全控制点变化—技术

安全控制点	旧标准	新标准的变化
网络架构	结构安全	修改为网络架构
通信传输	无	新增
边界防护	边界完整性检查	修改为边界防护
集中管控	无	新增
无	网络设备防护	删除
无	通信完整性	删除
无	通信保密性	删除
无	抗抵赖	删除
数据备份恢复	备份和恢复	修改为数据备份恢复
个人信息保护	无	新增

点击添加相关标题文字

安全控制点变化—管理

安全控制点	旧标准	新标准的变化
安全策略	无	新增
无	人员考核	删除
定级和备案	系统定级 系统备案	合并为定级和备案
无	监控管理和安全管理中心	删除
漏洞风险分析	无	新增
网络和系统安全管理	网络安全管理 系统安全管理	合并为网络和系统安全管理
配置管理	无	新增
外包运维管理	无	新增

测评项变化举例—网络和通信安全

安全控制点	旧标准测评项	新标准测评项的变化
网络架构	c）应在业务终端与业务服务器之间进行路由控制建立安全的访问路径。	删除
边界防护	无	d)应限制无线网络的使用，确保无线网络通过受控的边界防护设备接入内部网络。
入侵防范	无	c)应采取技术措施对网络行为进行分析，实现对网络攻击特别是未知的新型网络攻击的检测和分析。
安全审计	无	e)审计记录产生时的时间应由系统范围内唯一确定的时钟产生，以确保审计分析的正确性。
集中管控	无	a)应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控。
		b)应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理。
		d)应对分散在各个设备上的审计数据进行收集汇总和集中分析。
		f)应能对网络中发生的各类安全事件进行识别、报警和分析。

测评项变化举例—设备和计算安全

安全控制点	旧标准测评项	新标准测评项的变化
身份鉴别	a）应对登录操作系统和数据库系统的用户进行身份标识和鉴别。	a)应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换。
	b）操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换。	
	e）应为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性。	
	f）应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。	d)应采用两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术应使用密码技术来实现。
安全审计	无	f)审计记录产生时的时间应由系统范围内唯一确定的时钟产生，以确保审计分析的正确性。
剩余信息保护	a）应保证操作系统和数据库系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中。	删除
	b）应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。	

目录
CONTENT

网络安全远程技术检测

➢对北京市直属22家医疗机构及重点公共卫生机构的门户网站、APP、公众号信息系统进行了安全性远程技术检测

本次检测发现 22 个医疗单位

官网服务器共开放了 **55** 个端口

开放高危端口的官网服务器 **3** 个

15 家医院官网存在 **63** 个漏洞

高危漏洞 **13** 个

中危漏洞 **6** 个

低危漏洞 **44** 个

APP 检测共发现 4 个 APP 共发现了 36 个安全漏洞：

高危漏洞 **11** 个

中危漏洞 **6** 个

低危漏洞 **19** 个

公众号服务发现 3 处风险：

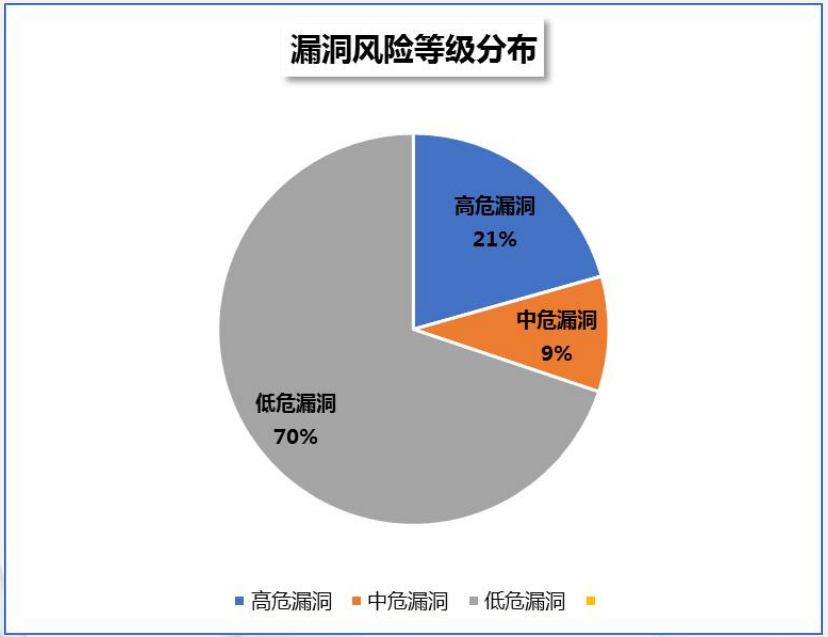
北京 114 预约挂号”公众号平台 **2** 个风险

“京医通”公众号 **1** 个安全风险

XX医院 **2** 个安全风险

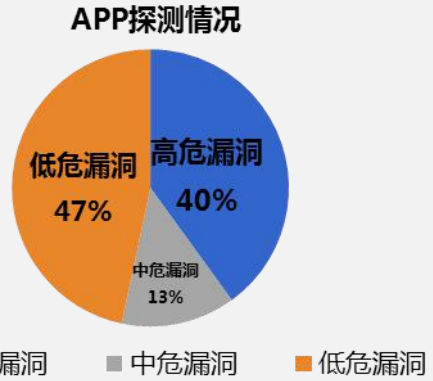
➢ 网络空间漏洞探测情况

- 共发现18种不同种类的漏洞，分布在15家医疗单位的22个官网域名上，共63个漏洞攻击入口，这63个漏洞中，有高危漏洞13个、中危漏洞6个，低危漏洞44个



➢ APP探测情况

- 共发现15种安全漏洞中，其中高危漏洞6个、中危漏洞2个，低危漏洞7个

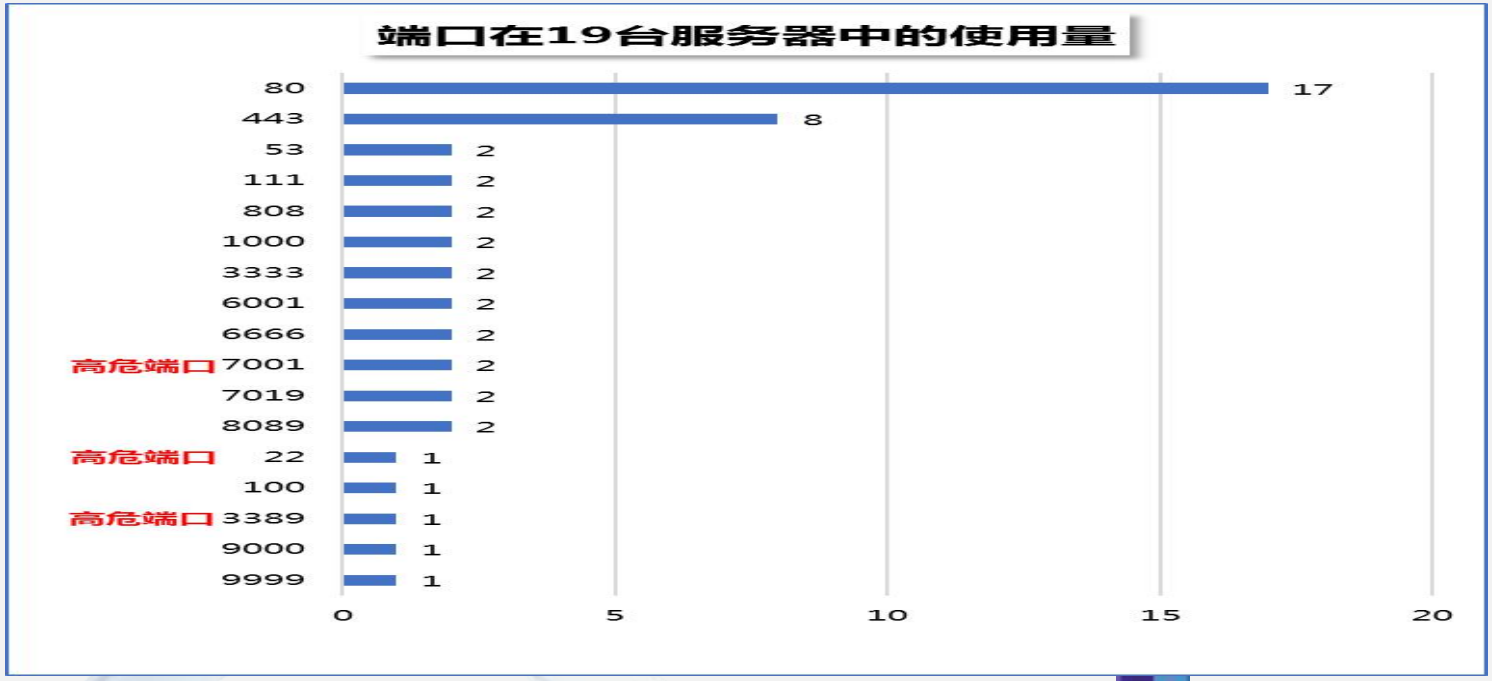


➢ 公众号检测情况

- 北京 114 预约挂号”：公众号平台 **2** 个风险
- “京医通”公众号 ：**1** 个安全风险
- XX医院 ：**2** 个安全风险

➢ 网站服务器开放端口情况

- 本次检测发现19台服务器上共开放了50个端口（涉及17个不同的端口）；
- 每个端口都是计算机对互联网的通信接口，开放过多不必要的端口会增加基础网络设施被攻击的可能；
- 17个不同端口在19台服务器中使用量如下：



➢ 网络空间高危漏洞情况

- 高危漏洞情况：本次探测共发现了4种高危漏洞，分布在3个网站服务器上。
- 高危漏洞是软件本身出现极其严重的漏洞，这些漏洞很容易被病毒、木马、黑客等侵入，导致软件崩溃或者盗取重要信息、密码等。
- 建议尽快修复安全问题，并做好安全管理工作，定期进行安全巡检，最大程度地避免安全问题

```
POST http://210.73.89.76/ServiceSelect/GridOrgInfoList HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: xmlHttpRequest
Referer: http://210.73.89.76/ServiceSelect/GetServiceSelectList#
Accept-Language: zh-cn
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Host: 210.73.89.76
Content-Length: 188
Connection: Keep-Alive
Pragma: no-cache
Cookie: ASP.NET_SessionId=yjrjmayreftxeqlldmfygril

ProductId=DATA10000000000011096911' and (select length(user) from dual)=8 aNd 's' lIke
's&OrgName=%E5%8C%97%E4%BA%AC%E5%AB%A3%E7%8A%D6%E5%A4%A9%E4%BD%DF%E5%8A%DF%E7%AD%A5%E5%8C%BB%E9%99%A2
```

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/json; charset=utf-8
Server: Microsoft-IIS/7.0
X-AspNetMvc-Version: 4.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Tue, 07 Aug 2018 07:02:52 GMT
Content-Length: 59

{"Data":[],"Total":1,"AggregateResults":null,"Errors":null}
```

➢ **APP检测详情：**各医院APP漏洞情况：15个漏洞的在4个医院APK中出现次数的情况：

漏洞名称	医院1	医院2	医院3	医院4
WebView组件系统隐藏接口未移除漏洞	9	9		
Android平台WebView控件跨域访问高危漏洞	1			
Android主机名\证书弱校验风险	12	16		
WebView File域同源策略绕过漏洞	2	2		
Webview绕过证书校验漏洞	14	13		
WebView控件AddJavaScriptInterface导致任意命令执行漏洞	2	1		
Android弱加密风险	3	1		
allowBackUp文件备份漏洞	1	3	1	1
Activity组件暴露风险	15	15	2	3
Service组件暴露风险	8	1	6	
ContentProvider组件暴露风险	1	13		
Broadcast Receiver组件暴露风险（含动态注册）	37	40	3	2
SendBroadcast信息泄漏风险	12	13		
Android应用拒绝服务漏洞	12	14		
ZIP文件解压目录遍历风险	4	3		

➢ 公众号探测情况

北京114预约挂号公众号平台

风险1类型：黄牛抢号风险

风险2类型：挂号业务风险，可挂取未开放挂号日期的号源

风险1描述：

风险解决方案：

京医通公众号平台

风险类型：页面异常，泄露服务器信息

风险描述：

解决方案：

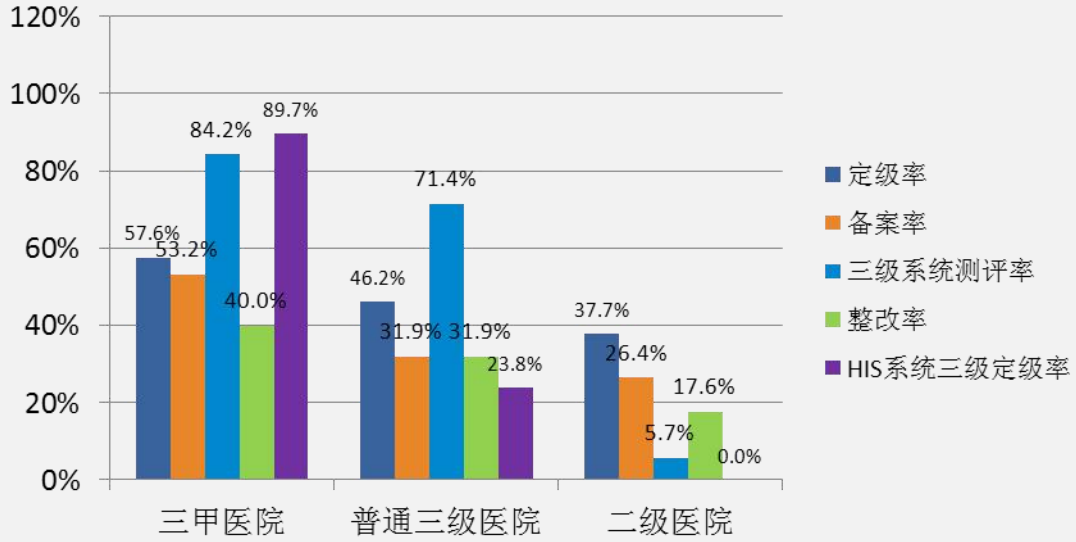
某医院公众号平台

风险类型：取消任意预约挂号

风险描述：

解决方案：

➢ 医院网络安全等级保护工作推进差异较大



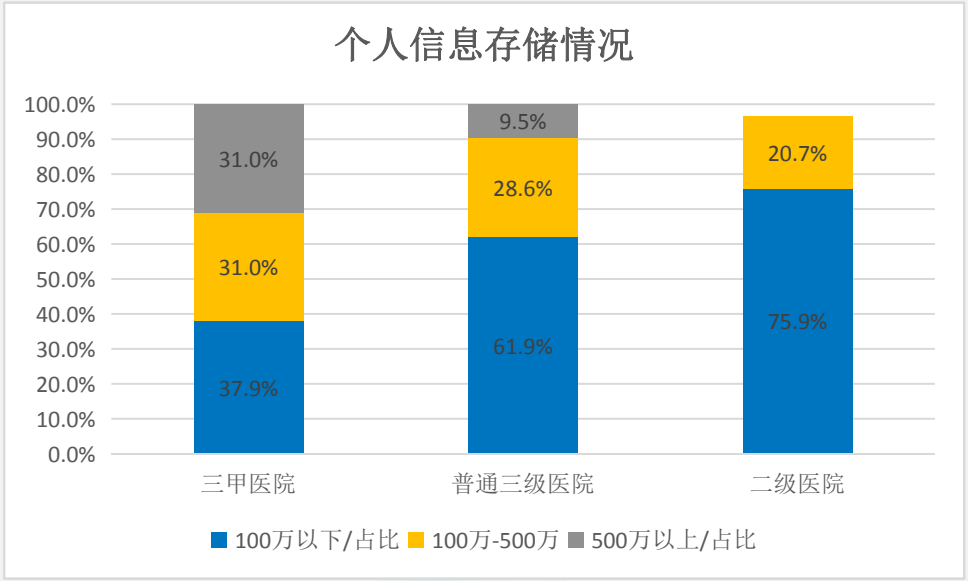
三甲医院信息系统整体定级、备案、三级系统测评、整改工作各项比率为57.6%、53.2%、84.2%、40%，HIS三级定级率为89.7%。普通三级医院信息系统整体定级率、备案率、三级系统测评率、系统整改率分别为46.2%、31.9%、71.4%和31.9%，HIS系统定为三级的比率为23.8%。二级医院信息系统整体定级率、备案率、三级系统测评率、整改比率分别37.7%、26.4%、5.7%、17.6%。

- ✓ 不同级别医院网络安全等级保护工作推进差异较大
- ✓ 三甲医院信息系统定级备案工作完成情况良好，对重要业务信息开展测评与整改工作方面力度较大
- ✓ 普通三级及以下医院（尤其是二级医院）的信息系统定级备案率远高于测评率、整改率
- ✓ 普通三级医院存在核心业务系统定级偏低（根据网络安全等级保护相关标准，结合系统调研数据中的个人信息存储量以及系统用户数）的情况
- ✓ 二级医院存在等级保护管理工作各环节衔接不到位的情况，网络安全等级保护工作推进的广度和深度不足。

调研结果分析

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

➢ 个人信息价值诱发更高安全风险



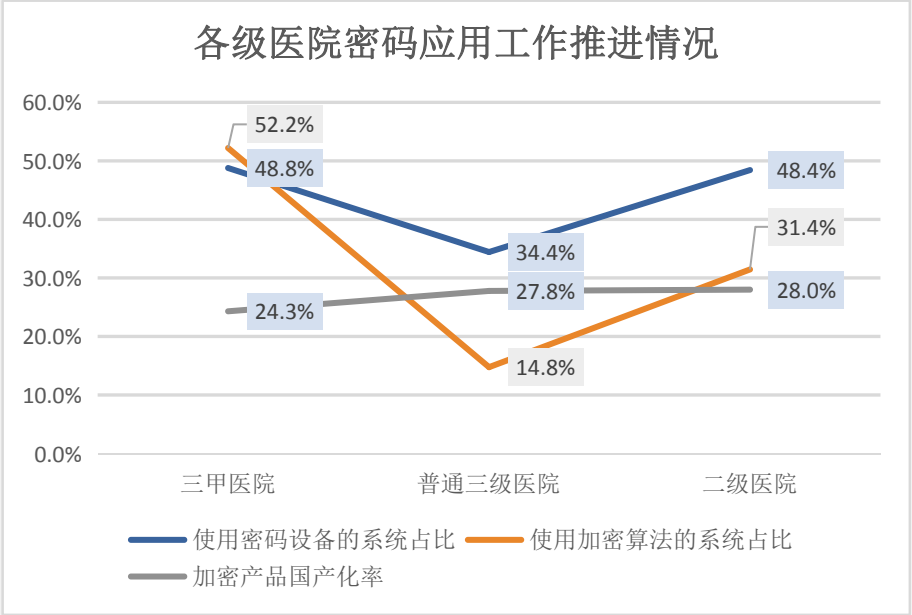
个人信息数据存储方面，行业内有62%的三甲医院、38.1%的三级医院和有24.1%的二级医院个人信息数据存储量达到100万条以上，

- ✓ 卫生行业涉及到大量的个人信息、医疗救治等隐私数据
- ✓ 等保2.0新标准规范在等保1.0的基础上特别提出了：需采取采用校验码技术或密码技术保证重要个人信息在传输和存储过程中的完整性和保密性；仅采集和保存业务必须的个人信息，并禁止未授权的访问
- ✓ 卫生健康行业在“互联网+医疗健康”发展中，其业务系统涉及大量个人信息采集、挖掘和利用和共享，在委个人就医带来了便利的同时，给个人隐私安全也带来了威胁

➢ 各级网络安全自主可控水平亟待提高

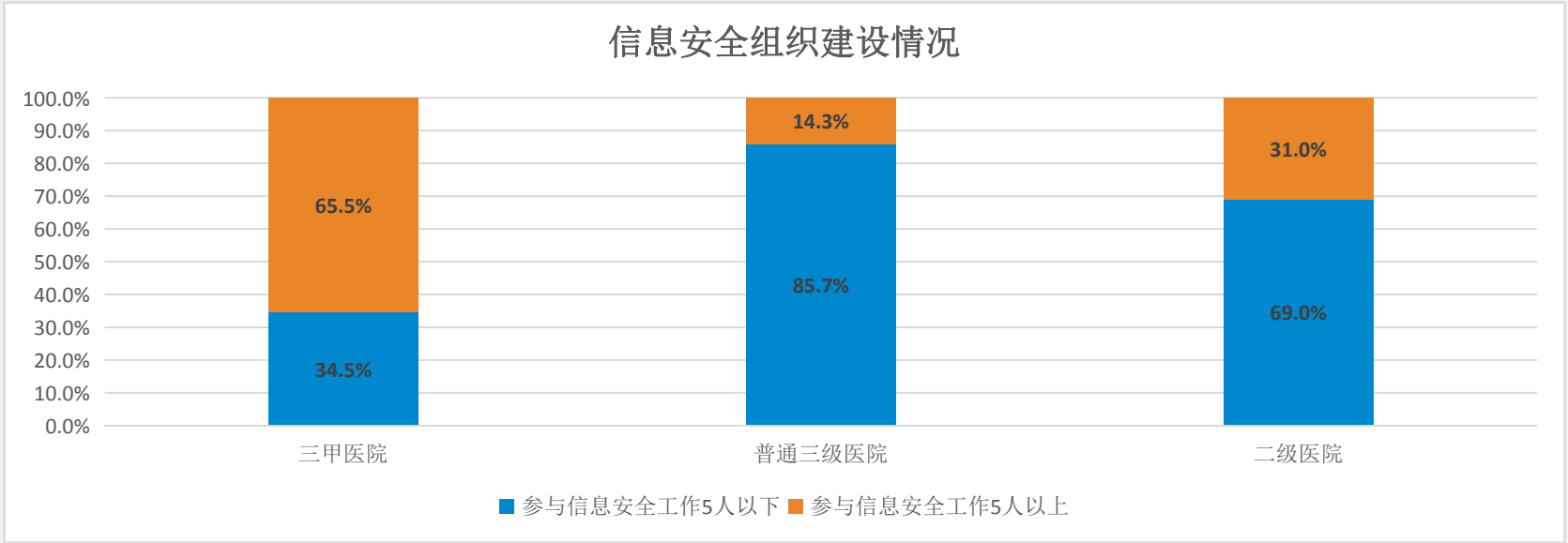
网络安全自主可控方面，从密码应用产品普及情况来看：

- ✓ 各级医院信息系统密码设备使用率，最高为48.8%；
- ✓ 加密算法使用率最高为52.2%，加密产品国产化率最高为28%；
- ✓ 而其他软件如操作系统、中间件和数据库等软件产品均使用国外产品，网络与数据的自主可控、安全防御水平亟待提高。

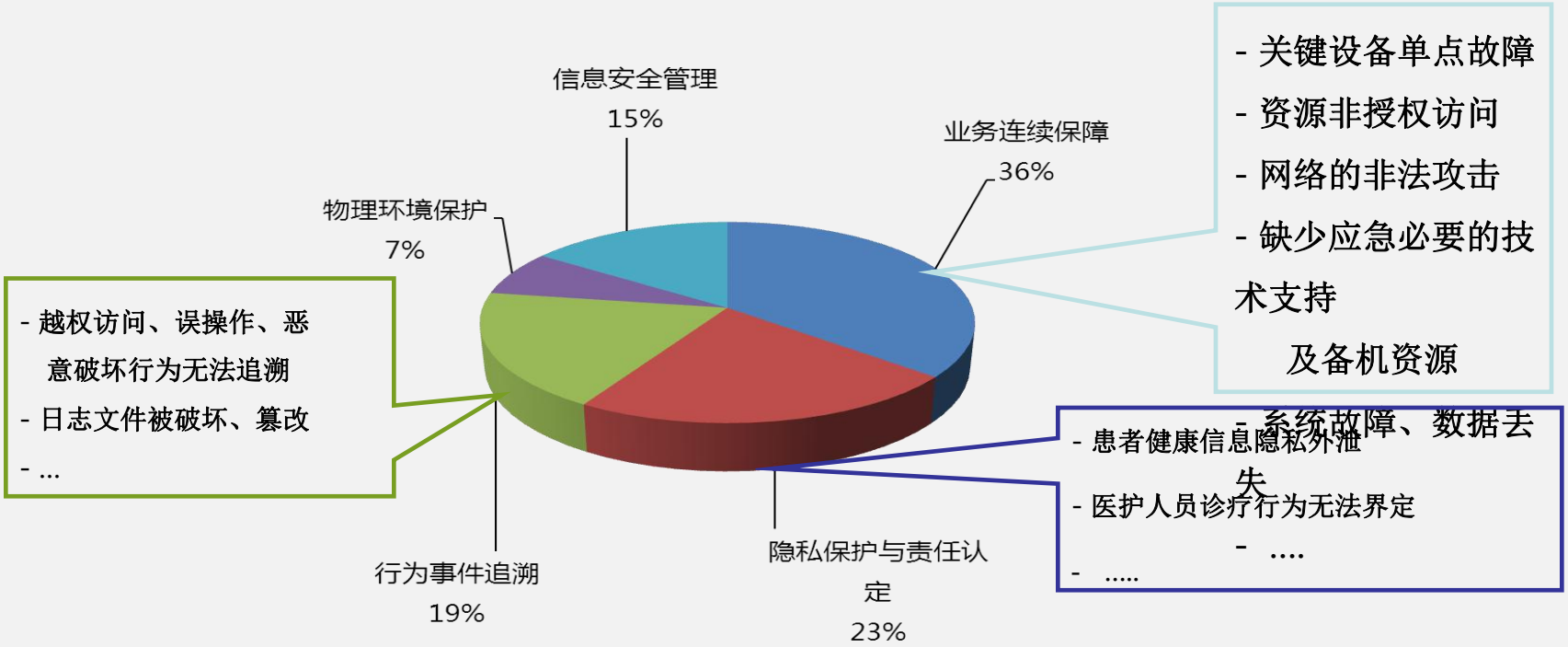


➢ 网络安全人员专业技能有待加强

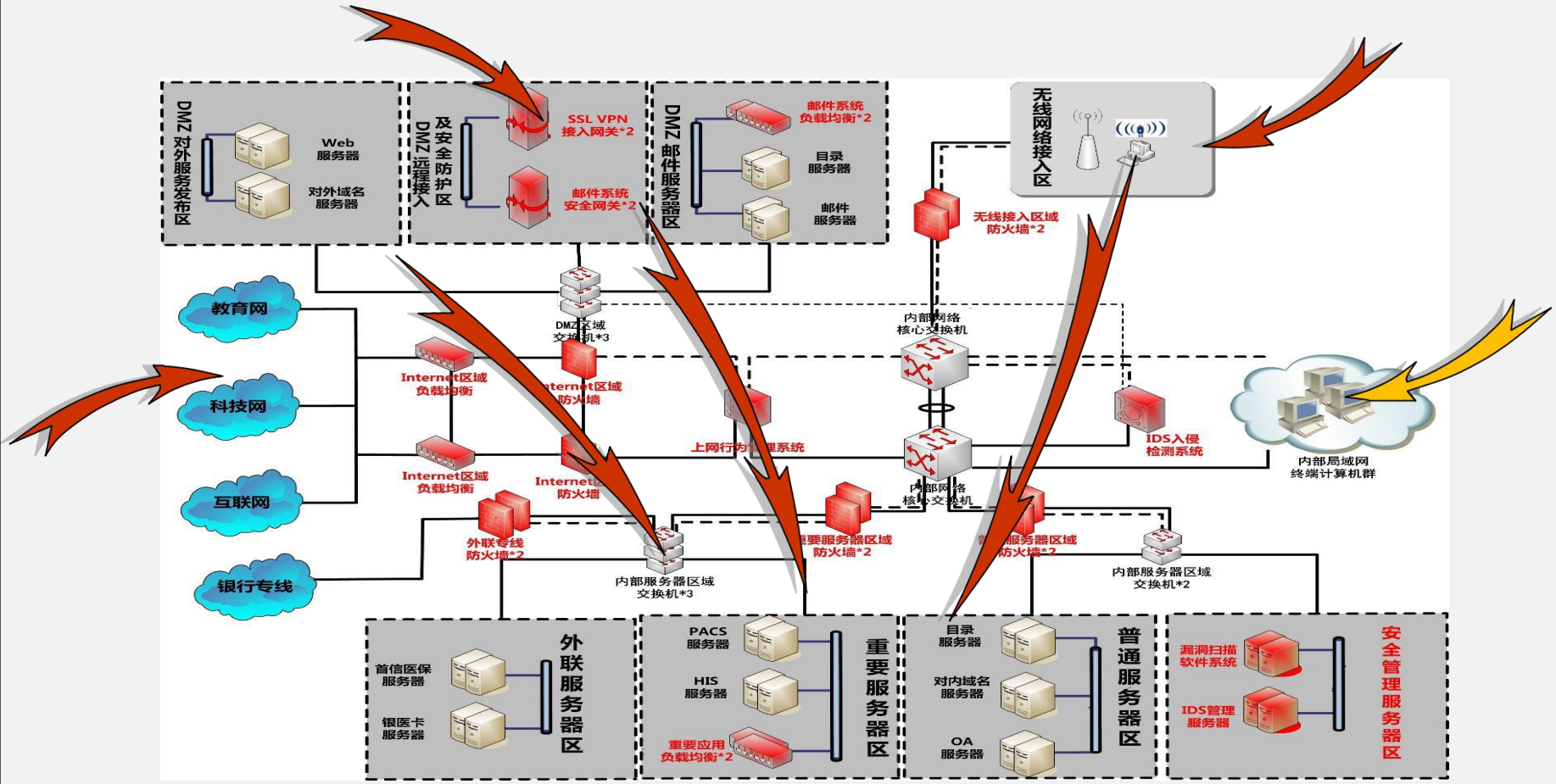
✓网络安全人员配备方面，虽然有65.5%的三甲医院、14.3%普通三级医院和31%的二级医院参与网络安全工作人员达到5人以上，但仍有**62.8%**的被调研单位认为**缺乏网络安全专业人员**是等级保护推进工作遇到的主要困难之一，由此可见，**参与网络安全工作人员网络安全专业知识和技能存在不足。**



医院信息系统存在诸多信息安全问题



互联网到内网核心的攻击路径演示



保密性：敏感信息保密性不足，可遭泄露

患者信息

- 基本信息（姓名、身份证号、家庭地址等）、住院信息、电子病历信息
- 侵犯个人隐私，易造成舆论压力或影响

医疗信息

- 医生处方、医嘱等信息
- 侵犯医生知识产权

人种信息

- 大量具有研究意义的患者信息
- 被国外研究机构或不法分子获取，可分析群体身体状况，甚至危及国家安全

可用性：系统被控制，业务可被中断

业务中断

- HIS、LIS、PACS、UIS系统及服务器
- 业务系统中断，无法就诊

扰乱秩序

- 排队叫号系统
- 打乱顺序，激化医患矛盾，扰乱正常医疗秩序

群体事件

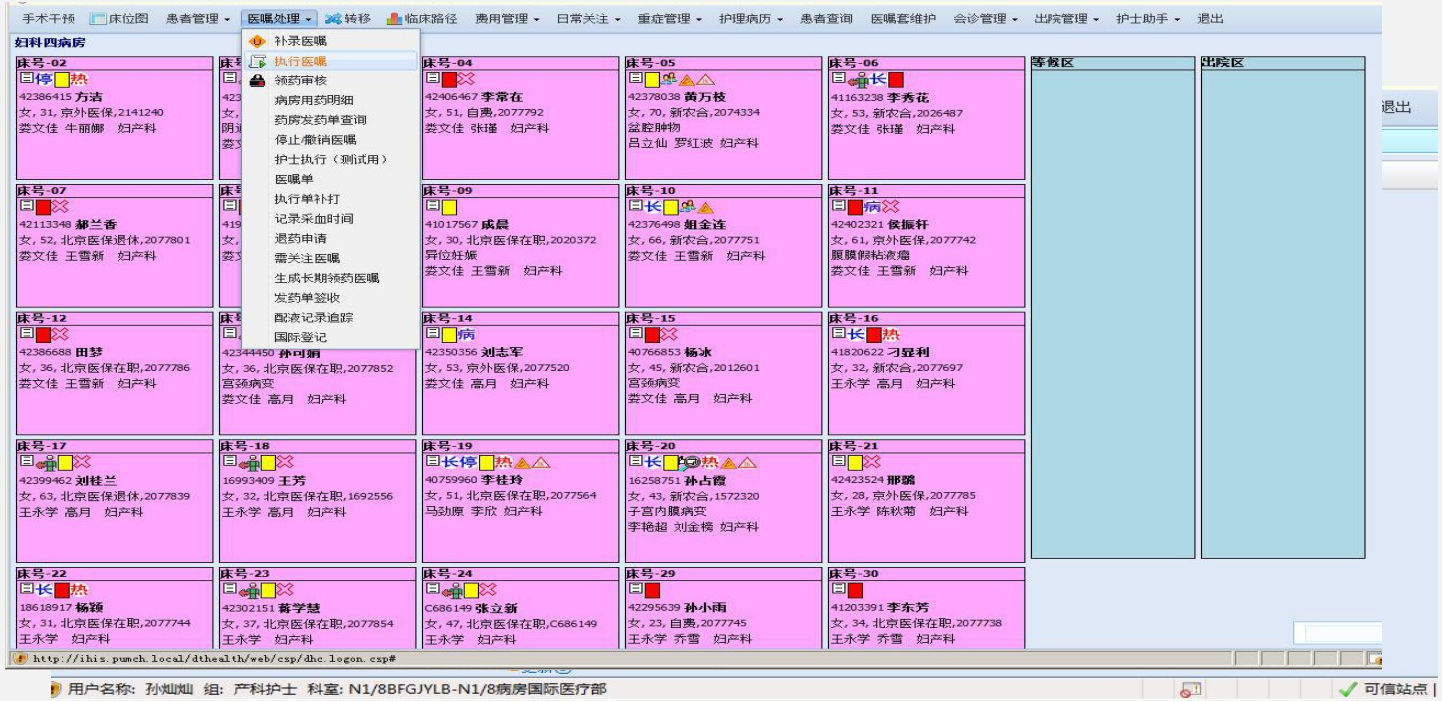
- 媒体发布系统（大屏幕）、门户网站
- 发布反动、虚假等不良信息，引发群体性事件

可用性：系统被控制，业务可被中断

- HIS系统、自助终端（挂号、缴费、查结果等）

完整性：数据完整性校验不当，可篡改

- 办出院
- 改医嘱
- 调剂量

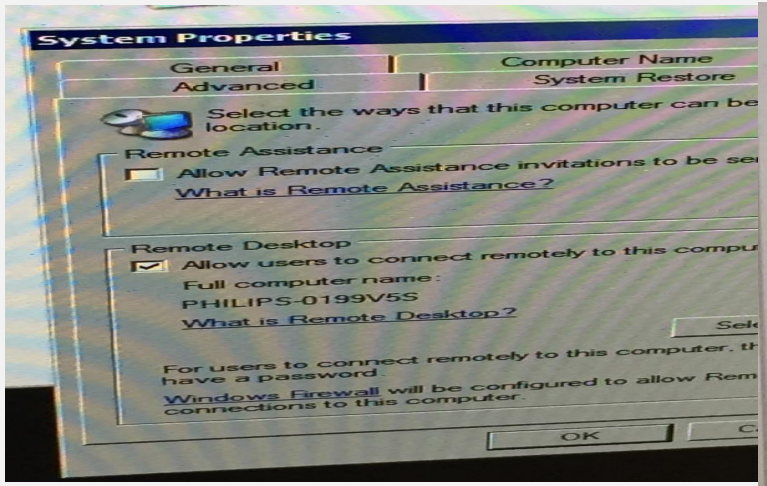


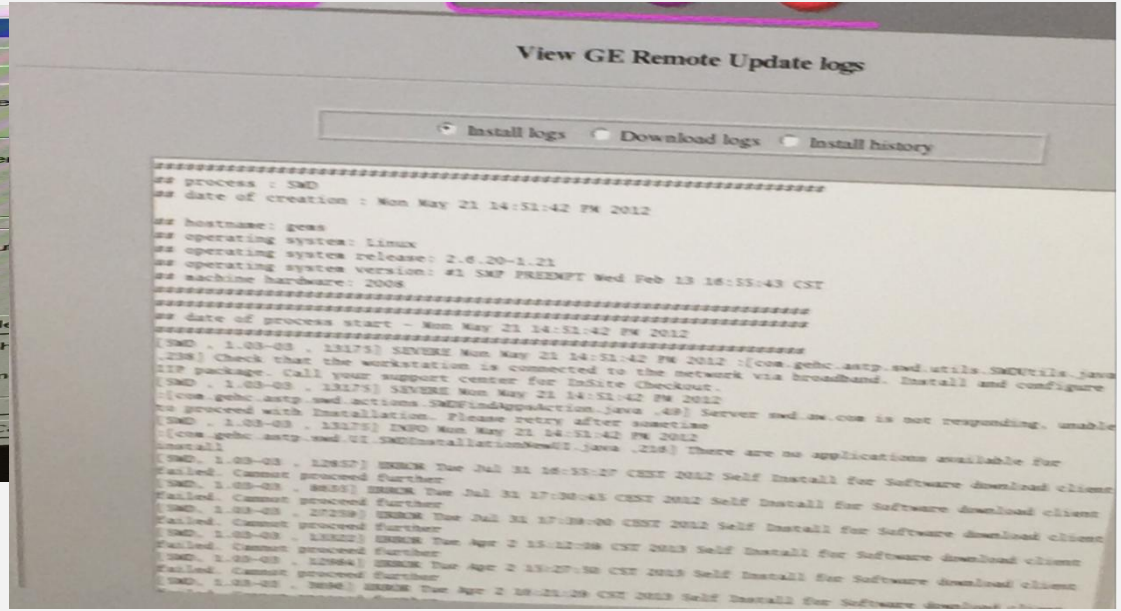
自主可控：依赖国外产品现象突出

- 大型医疗设备（核磁、CT等）在重要大型部属医院中依赖国外产品现象十分突出。
- 运维全部依靠厂商，权限外泄严重。
- 设备本身的安全隐患医院无从知晓，缺少国家统筹的前置性安全检测
- 底层操作系统开放了过多不必要的端口(3389等)
- 预留了插3G上网卡的接口，虽未使用，但存在非法外联的隐患

自主可控：无国产化

- 设备均支持远程维护，存在数据泄露安全隐患。
  - 设备默认将会在本地存储大量患者照片信息存在通过FTP、USB设备导致数据泄露的隐患。





医院网络安全状况总体评价

- 我国医院现有的安全保障体系尚处于初步建设阶段，其安全状况和防护能力尚不足以应对当前网络安全威胁，不足以保证信息系统的安全稳定运行，**难以抵御一般性有组织的网络攻击行为，**行业整体网络安全保障水平亟需提升。

目录
CONTENT

- 加强网络安全等级保护工作重视程度

- **习近平总书记提出“没有网络安全就没有国家安全”。**
- 《网络安全法》中也明确规定“国家实行网络安全等级保护制度”，而卫生健康行业作为国家重要行业与领域，其网络安全关乎到国计民生和公共利益。行业各单位应积极落实网络安全制度，领导层也应提高网络安全等级保护工作的认知水平和重视程度，应理解网络安全等级保护工作开展意义与重要性，确保网络安全等级保护工作推进工作顺利开展。

- 明确本单位负责网络信息与数据安全工作的职能部门，负责建立本单位的网络信息与数据安全管理制度和操作规程，明确网络信息与数据系统、互联网服务、应用平台建设和运维管理等过程中的网络信息与数据安全责任。
- 按照网络安全法、网络安全等级保护及相关要求开展网络信息与数据安全体系建设，坚持网络安全与信息化建设项目“同步规划、同步建设、同步运行”的原则，开展信息系统定级备案，定期开展等级测评和风险评估，选取符合资质要求的技术支撑机构和健康医疗服务企业，保障日常工作的安全开展。

- 在保障网络安全的基本前提下，加大对自主可控产品的使用与投入，有计划、有步骤地实现行业网络安全产品国产化替代，使用符合国家要求的密码产品，实现信息化与信息系统安全技术与产品自主可控和安全可信，提高行业网络安全自主可控水平。
- 扩充网络安全队伍，提升网络安全队伍专业技能，强化单位人员安全意识。根据信息化建设规模及日常网络安全保障需求，逐步增加网络安全专业力量，持续性开展本单位网络安全培训工作，提升网络安全从业人员在安全设备维护管理、网络安全监控、系统安全审计、漏洞及风险管控、病毒查杀、数据备份恢复、应急处置等方面的技能。

- 履行业务和信息系统的安全保障义务，开展信息系统安全运维，定期开展完全检查，对存在的漏洞、隐患或计算机病毒等及时进行整改，杜绝网络信息与数据安全事件的发生。

- 建立本单位网络信息与数据安全应急体系，制定应急预案、组建应急队伍、开展应急演练。发生网络信息与数据事件时，依照预案进行事件处置并将相关情况上报卫生健康行政部门的同时，报网络安全主管部门。

- 履行相关法律法规规定的其他责任，组织本单位工作人员开展网络信息与数据技术安全教育与培训，落实相关管理部门的工作部署，保障必要的经费投入。
- 根据国家个人信息保护相关法律规定、等保2.0安全标准，从个人信息的采集、传输、存储、加工和应用过程等多方面加强个人信息数据保护，有效落实数据加密存储及传输、个人信息去标识化、数据防泄露等安全防护措施，确保个人信息合法使用和得到有效保护，防止个人信息的泄露和滥用。

谢 谢