
# 医院信息安全调查报告

中国医院协会信息专业委员会

2019 年 3 月

# 目录

## 一、 调查背景

当前，伴随信息技术的飞速发展，信息化和网络化建设已经成为我国社会经济活动的基础保障，面对日益增加的安全风险，网络安全建设工作上升为国家战略高度。在医疗健康领域，随着医院信息化的普及和深入，信息系统成为医院运营核心技术支撑，特别是深化医药卫生体制改革以来，医院业务从院内走向院外，从封闭走向开放，医院信息系统面临着前所未有的新风险。在医院业务持续性方面，医院信息系统面临的病毒、木马、网络泄露等安全威胁风险越来越高，网络信息安全责任重大。在医疗数据安全方面，患者信息隐私保护以及数据完整性安全建设亟需得到加强。医疗行业的数据安全形势日趋严峻。

国家行业管理部门高度重视医疗机构网络和信息安全工作，2011 年，国家卫生健康委员会（原国家卫生部）印发了《卫生行业信息安全等级保护工作的指导意见》，要求医疗卫生机构依据国家信息安全等级保护制度，遵循相关标准规范，进行信息安全等级保护定级备案、建设整改和等级测评等工作。2014 年，国家卫生健康委员会（原国家卫生计生委）发布《人口健康信息管理办法（试行）》，对人口健康信息安全和隐私保护工作提出要求。2017 年 6 月 1 日开始实施的《中华人民共和国网络安全法》，明确将国家网络安全等级保护制度上升为法律要求。2018 年 6 月，公安部发布《网络安全等级保护条例（征求意见稿）》，将网络安全等级保护扩展到云计算、大数据、物

联网、移动互联网以及公共新领域，推动网络安全等级保护进入“2.0”时代。作为国家卫生健康行业信息化建设的重要保障和重要组成部分，医疗行业网络信息安全工作迈入了新的发展阶段。

为了掌握我国医院信息安全建设现状，评估信息安全工作水平，发现信息安全薄弱环节，为医院制定信息安全建设规划提供帮助，中国医院协会信息专业委员会(原信息管理专业委员会，以下简称 CHIMA)2018 年底开始对我国部分医院信息安全建设情况进行了调查，通过数据清理和汇总分析，编写了《CHIMA 2019 医院信息安全调查报告》，供医疗行业管理部门、医疗机构和信息安全厂商提供决策依据。

本次调查没有采用随机分层抽样的方法，数据由各医院自愿参加填写。限于 CHIMA 的资源与经验，本次调查报告存在着许多不足、缺陷，希望得到业内同行与广大读者的批评指正。

## 二、 调查基本情况

### （一） 调查工作依据

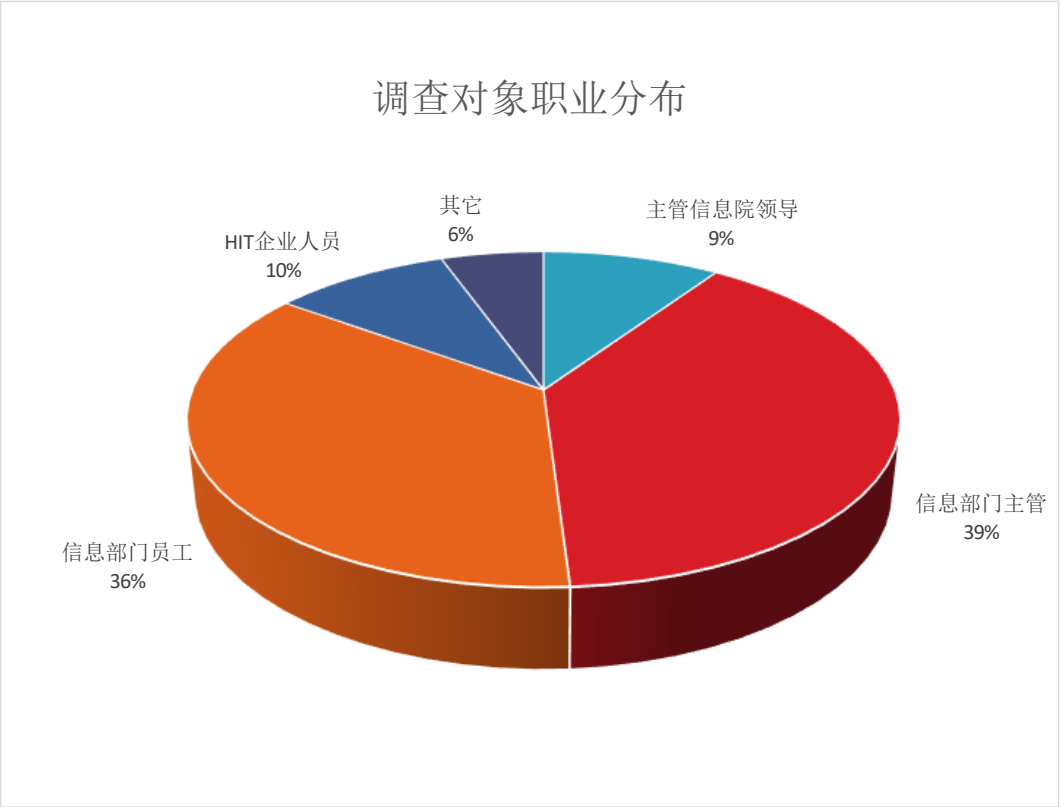
此次调查工作参考依据如下：

- 《中华人民共和国网络安全法》
- 《国家网络空间安全战略》
- 《网络安全等级保护条例》（意见征求稿）

- 《信息安全技术 网络安全保护等级定级指南》（GA/T 1389—2017）
- 《信息安全技术 网络安全等级保护基本要求》（送审稿）
- 《个人信息保护法》（专家意见稿）
- 《信息安全技术个人信息安全规范》
- 《全国医院信息化建设标准与规范》

## （二） 调查对象

本次调查受访者共计 400 人，以医院信息化工作者为主，占总受访人群的 86.75%。其中，主管信息院领导为 38 人，占比 9.5%;信息部门主管 158 人,占比 39.5%;信息部门员工 144 人，占比 36%。另外，HIT 企业人员占 10%，其他 6%。




## （三） 调查方式

本次调查采用问卷调查形式，在全国范围内通过网络调查的方式开展了为期一个月的医疗卫生机构信息安全调查。

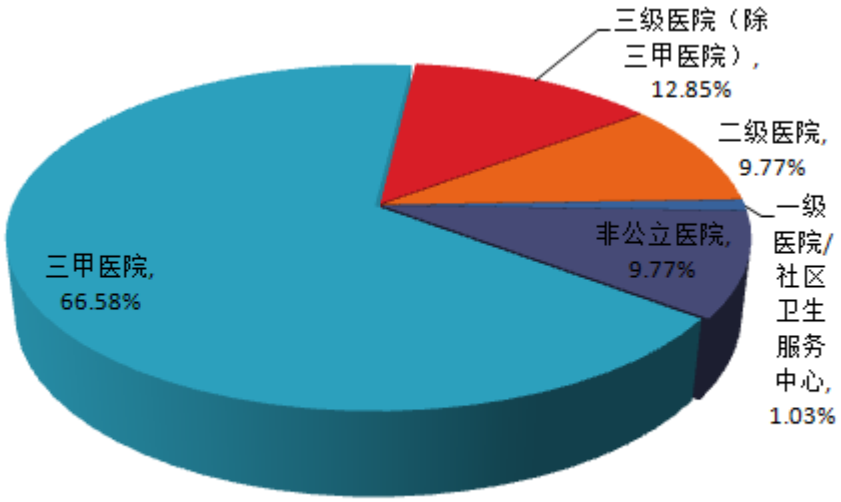
本次调查采用公开问卷，各省、市、自治区卫生行政部门、医院和CHIMA CIO俱乐部组织自愿参加、电话跟踪的调查方法。

## （四） 调查内容

本次调查内容包括：调查对象基本情况、近三年信息化建设情况、等级保护制度落实情况、信息安全建设投入和产出情况，以及信息安全工作计划和采购意愿等调查内容。

## （五） 调查分布

本次调查共回收有效问卷 400 份，医院样本总数为 389 家，覆盖了 29 个省、直辖市（包含中国台湾省），医院占总参与调查机构的 97.25%。其中：三甲医院为 259 家，在受访医院中占 66.58%；三级医院（除三甲医院）共有 50 家，占比 12.85%；二级医院有 38 家，占比 9.77%；一级医院 / 社区卫生服务中心 4 家，占比 1.03%；非公立医院 38 家，占比 9.77%。



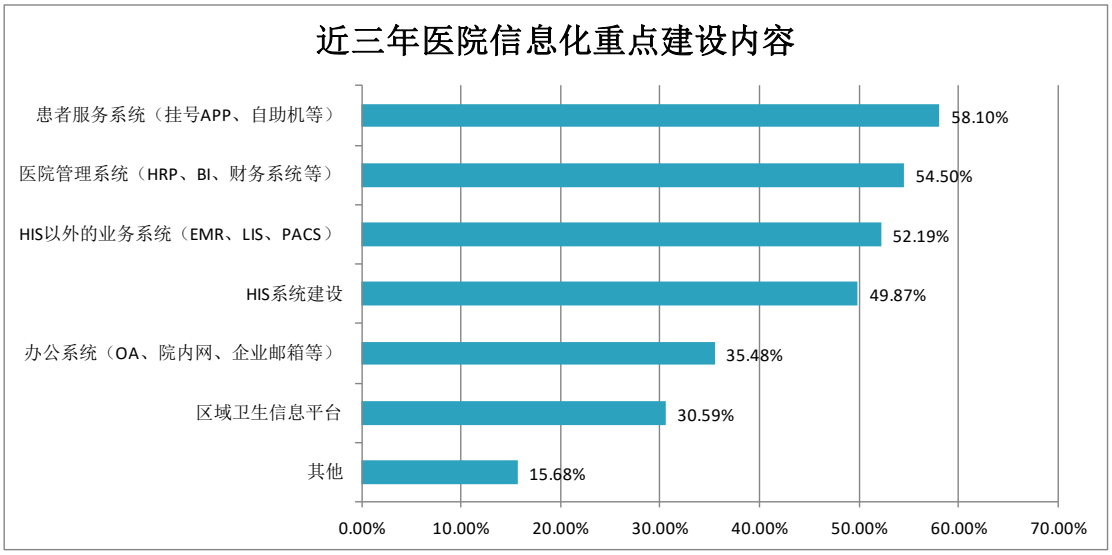

# 三、 调查结果

## （一） 近三年医院信息化重点建设内容

近些年，新的 IT 技术的发展和应用，加速了医院信息化的发展和相关产品技术的创新，但不同医院信息化建设发展阶段有差别，医院信息化建设重点各有不同。

本次调查显示，在近三年医院信息化建设重点内容的调查排名前三位的是，重点建设患者服务系统（挂号 APP、自助机等）

的医院为 226 家，占比 58.10%，重点建设医院管理系统（HRP、BI、财务系统等）的医院为 212 家，占比 54.50%，重点建设 HIS 以外的业务系统（EMR、LIS、PACS、超声等）的医院为 203 家，占比 52.19%。



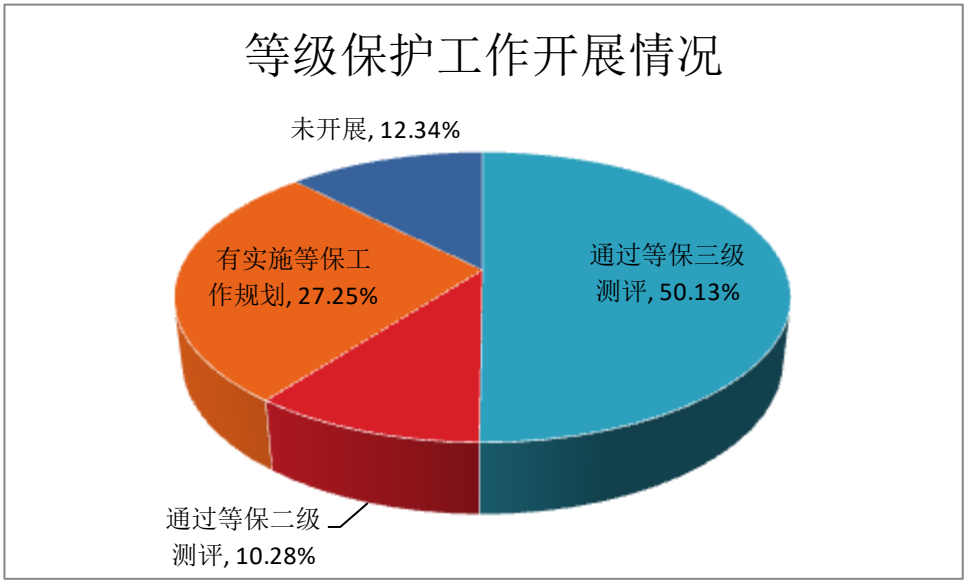

由此可看出，随着医院以患者为中心服务理念的逐步落地，患者服务系统已成为近年来及下一步医院信息化建设的首要重点之一。同时，医改政策的实施和医院绩效考核的加强推动越来越多医院将建设重点转向医院管理系统（HRP、BI、财务系统）等，助推医院实现精细化管理。随着医院 HIS 系统的普遍应用，EMR、LIS、PACS 等系统的建设也提到了大部分医院的日程中来。

## （二） 等级保护工作开展情况

随着信息技术的不断发展，特别是云计算、4G/5G、物联网等新技术的不断涌现和应用，在带给医疗行业快速、便捷的同时，也让安全风险变得没有边界，开展等级保护工作面临着越

来越多的新情况、新问题。国家卫生主管部门对医疗机构的信息安全等级保护工作提出了严格要求。通过等级保护测评工作，发现医院系统内、外部存在的安全风险和隐患，提高信息系统的信息安全防护能力，降低系统被各种攻击的风险，能够更加有效的保障医疗信息安全。

通过此次调查发现，至少有一个系统通过等保三级测评的受访医院共计 195 家，占比 50.13%；通过等保二级测评的受访医院共计 40 家，占比 10.28%；有实施等保工作规划的医院有 106 家，占比 27.25%；没有开展等保工作规划的医院有 48 家，占比 12.34%。

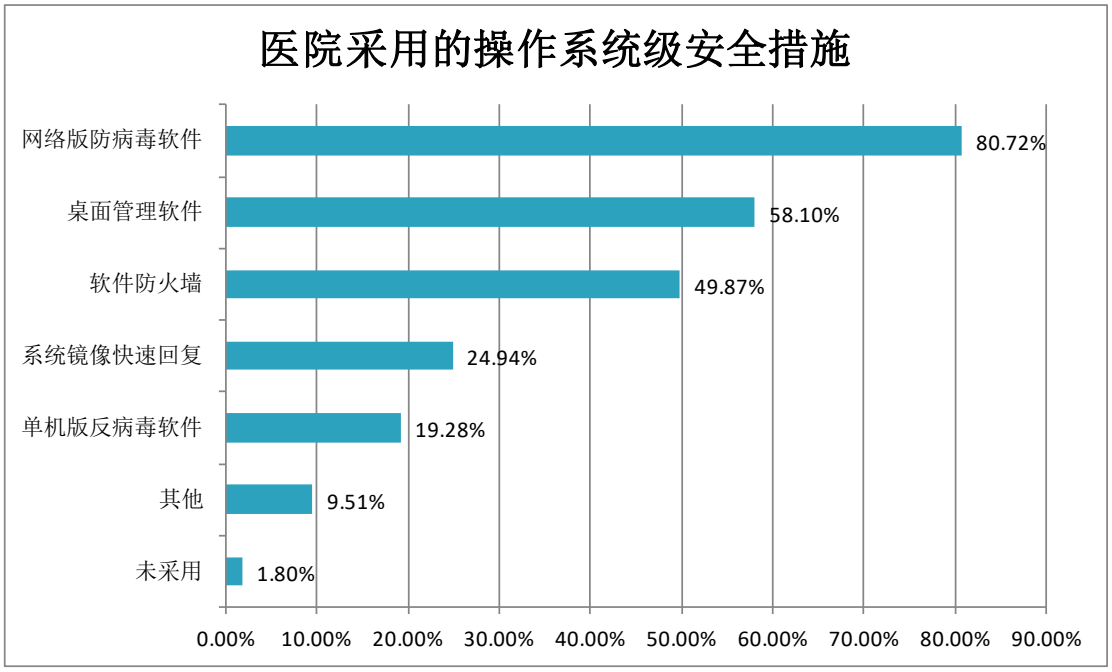



调查发现，目前等级保护测评在医院的普及率还不高，仍有很大进步空间。等级保护有助于对系统安全进行重新梳理，提高工作人员的安全意识和处理安全事件的能力。因此，医院在信息化建设中适当提高对等级保护的侧重，有助于保障医院

信息系统持续稳定运行。

## （三） 操作系统级安全措施

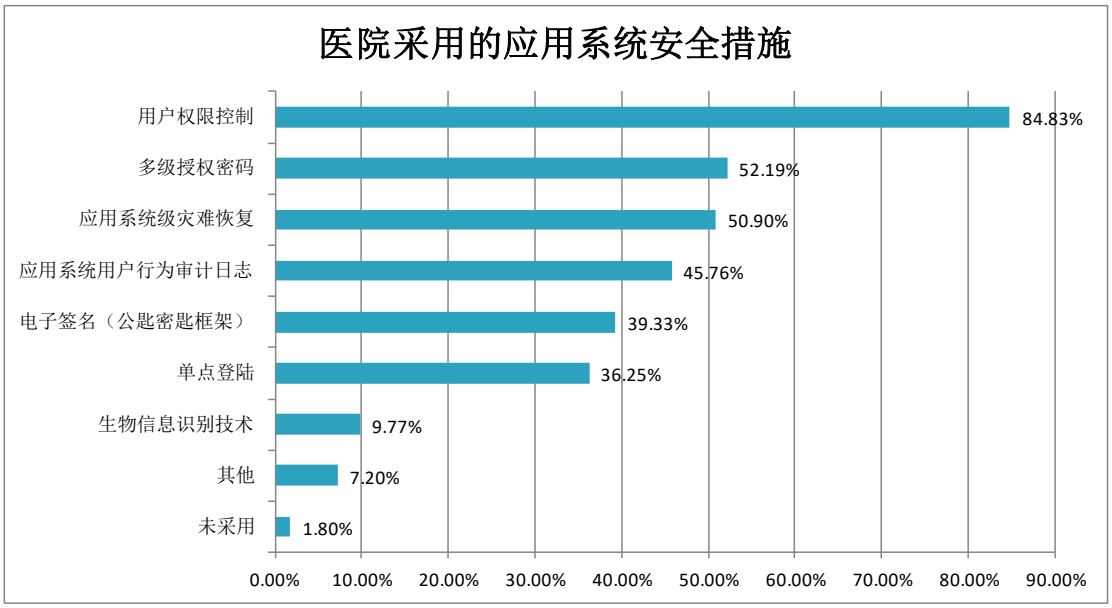
在对操作系统级安全措施的调查中发现，上线网络版病毒软件的医院共计 314 家，占比 80.72%；上线桌面管理软件的医院共计 226 家，占比 58.10%；上线软件防火墙的医院共有 194 家，占比 49.87%；未采用任何措施的医院仍有 7 家，占比 1.80%。




由此可看出，目前医院对操作系统级的安全防护方式仍以网络版防病毒软件为主，但有少部分医院甚至没有采取操作系统安全防护。随着勒索病毒、黑客等网络攻击手段的不断变化，医院在操作系统防护方面应适当增加一些新的安全技术，多重防护。

## （四） 应用系统级安全措施

在应用系统级安全措施方面，排名前三位的分别是：用户权限控制、多级授权密码以及应用系统级灾难恢复。其中采取用户权限控制的医院共有 330 家，占比 84.83%；采用多级授权密码的医院是 203 家，占比 52.19%；应用系统级灾难恢复的医院共有 198 家，占比 50.90%。

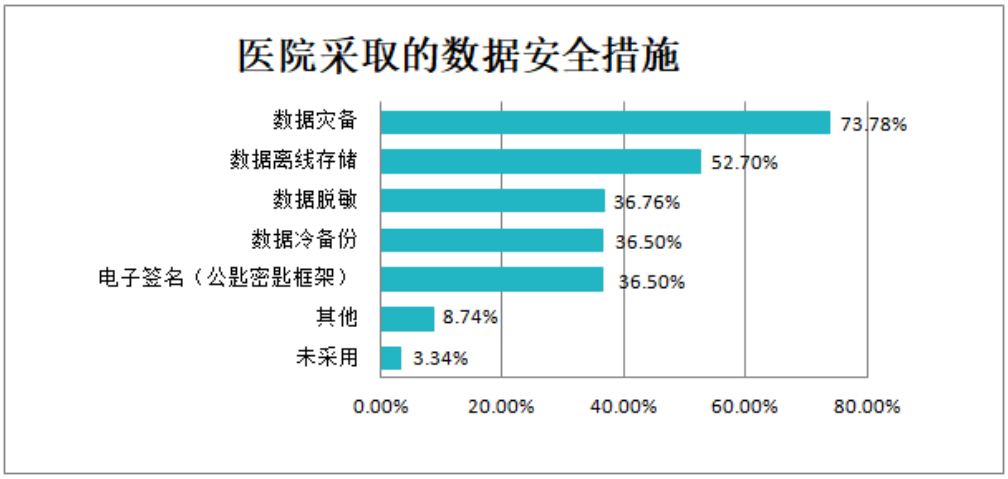



从调查情况可看出，用户权限控制仍然是医院保障系统级安全常用措施。同时，数据显示，未采用安全措施的绝大部分为非公立医院。

## （五） 数据安全措施

在大数据时代，切实保障医疗数据安全成为焦点。通过此次调查发现，开展数据灾备的医院共有 287 家，占比 73.78%；采取数据离线存储的医院共有 205 家，占比 52.70%；进行数据脱敏的医院共计 143 家，占比 36.76%；未采取数据安全保障措

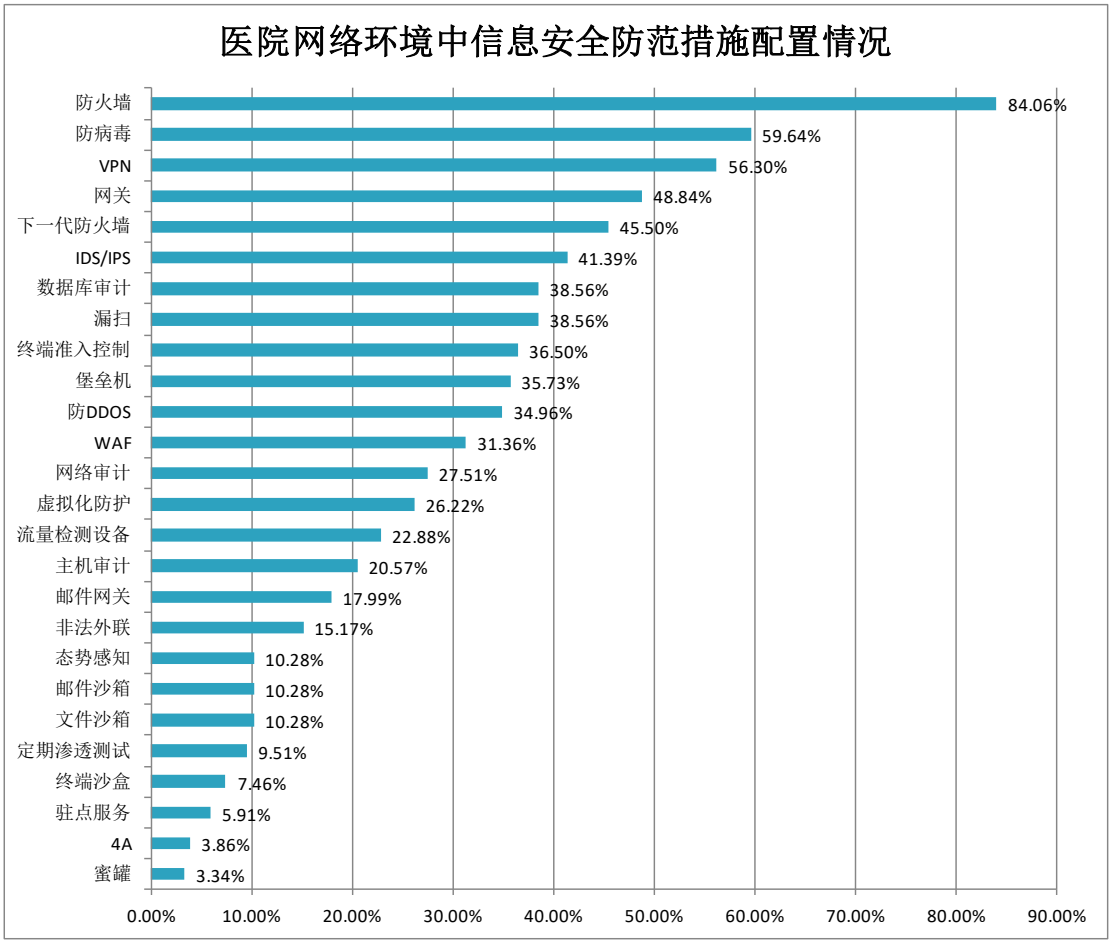
施的医院仍有 13 家，占比 3.34%。




医疗数据安全是医疗大数据要面对的主要问题之一。从统计情况中发现，数据灾备、离线存储得到了受访医院一半以上的认同和应用。但仍然有少部分医院没有采取任何防控措施。

## （六） 网络安全防范措施

医院网络安全防范措施的应用情况是本次调查的重要内容之一。在网络环境中，为防止患者个人隐私数据丢失、篡改、泄露或损坏，医院采取了系列信息安全防范技术措施，包括设置防火墙、安装防病毒软件、配置 VPN 等。在本次调查中，网络安全防范措施排名前三位的分别是：设置了防火墙的医院共有 327 家，占比 84.06%；上线防病毒软件的医院共计 232 家，占比 59.64%；配置 VPN 的医院共有 219 家，占比 56.30%。

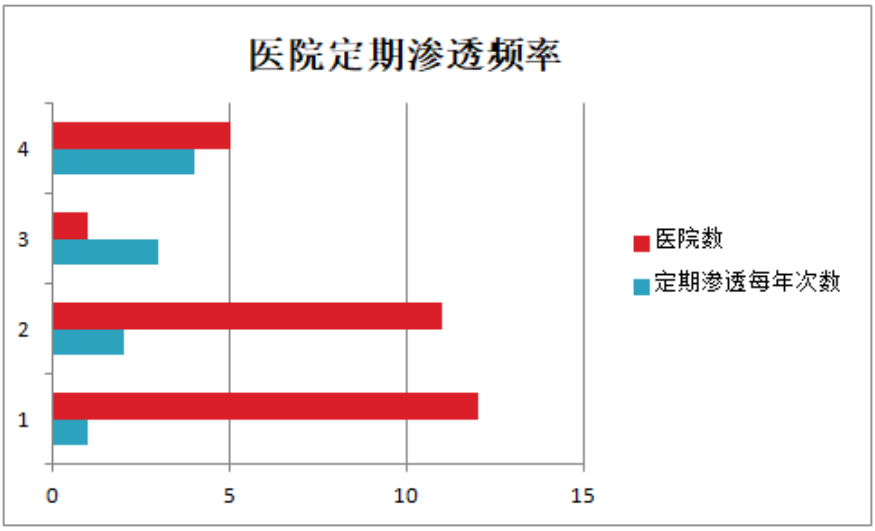



调查显示，目前医院对网络安全重视程度已大幅提高，采取多项措施保障网络安全。不过，调查显示仍有少部分医院未做基本的网络安全防护或防范形式单一，使网络面临风险。

## （七） 渗透测试工作开展情况

在医院信息网络安全工作中，采取定期渗透的方式对系统进行测试是一个有效手段。本次调查对医院定期渗透频率进行了摸底，共有 37 家受访医院表示采用了定期渗透测试以保障信息安全，占总受访医院的 9.51%。这 37 家医院中有 29 家填写了定期渗透的每年次数。结果显示，每年做一次定期渗透的医院有 12 家；每年做两次定期渗透的医院有 11 家；每年做三次

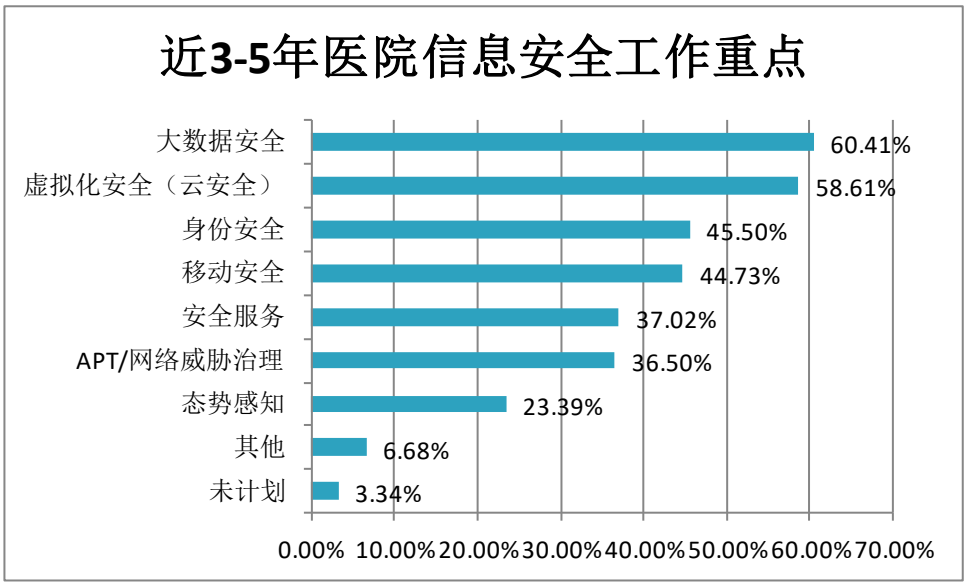
定期渗透的医院有 1 家；每年做四次定期渗透的医院共计 5 家。




由此可见，医院对信息系统开展定期渗透测试的重要性未得到重视，网络渗透测试的频率偏低。

## （八） 信息安全工作重点

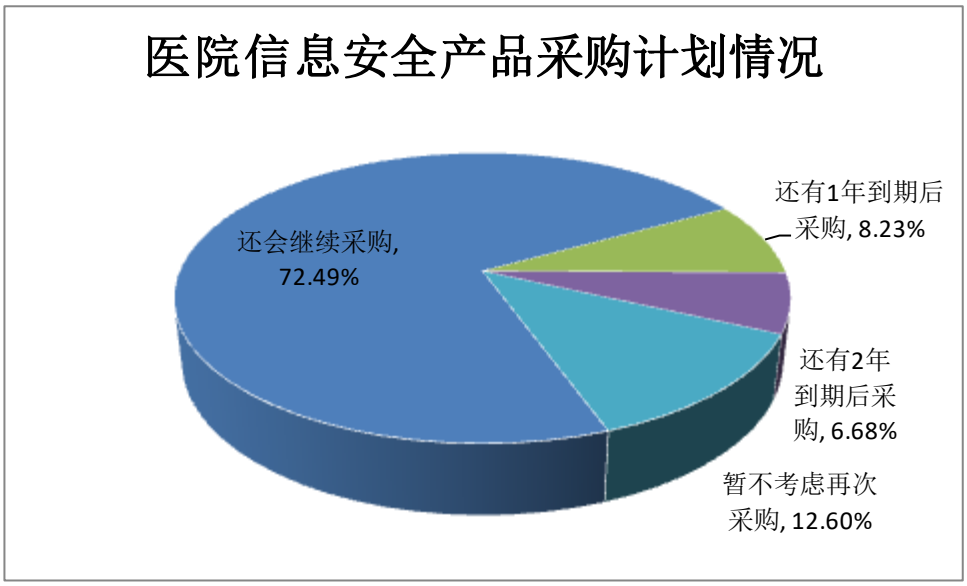
针对未来 3-5 年医疗信息安全的工作重点这一议题，共计 235 家医院选择的是大数据安全，占比 60.41%；228 家医院计划上线虚拟化安全（云安全），占比 58.61%；177 家医院将进行身份安全认证，占比 45.50%；174 家医院将采取措施保障移动安全，占比 44.73%；另有 13 家医院对近 3-5 年信息安全保障工作的重点还未有明确计划。

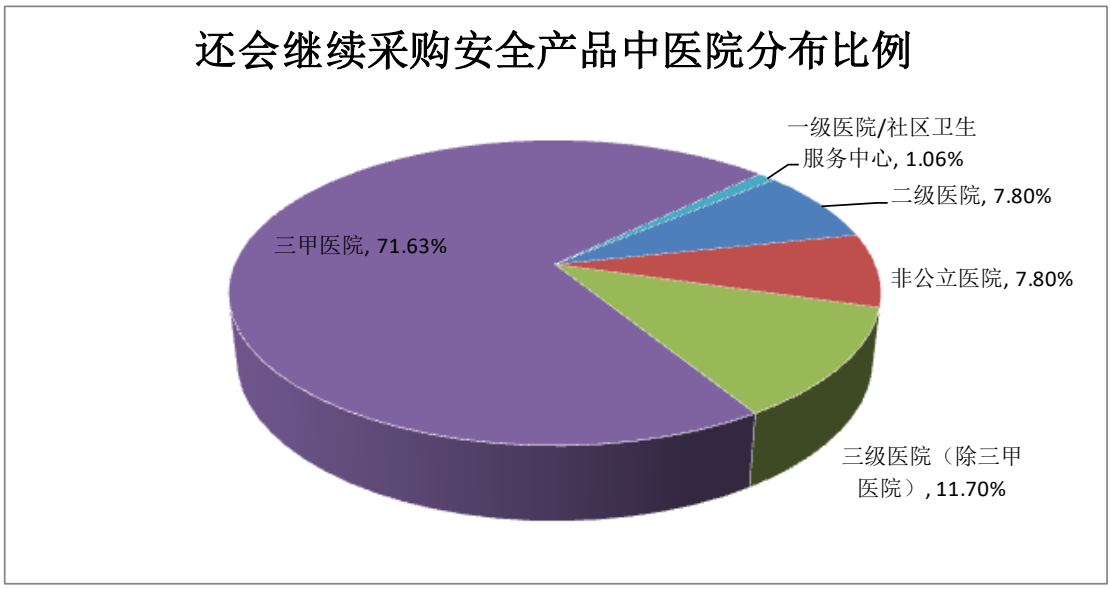



调查结果显示，大多数医院重视加强信息安全工作，从加强大数据安全、虚拟化安全等多方面入手。同时，仍有少数医院仍处在观望态度，对信息安全保障的规划尚不明确。

## （九） 信息安全产品采购计划情况

针对未来医院是否持续采购医疗信息安全解决方案这一选题，282 家受访医院选择会继续采购，占比 72.49%，其中三甲医院占选择会继续采购医院总数的 71.63%，占总受访医院的 51.93%；32 家受访医院表示会在 1 年后采购，占比 8.23%；26 家受访者选择会在 2 年后采购，占比 6.68%；另有 49 家表示暂不考虑再次采购，占比 12.60%。



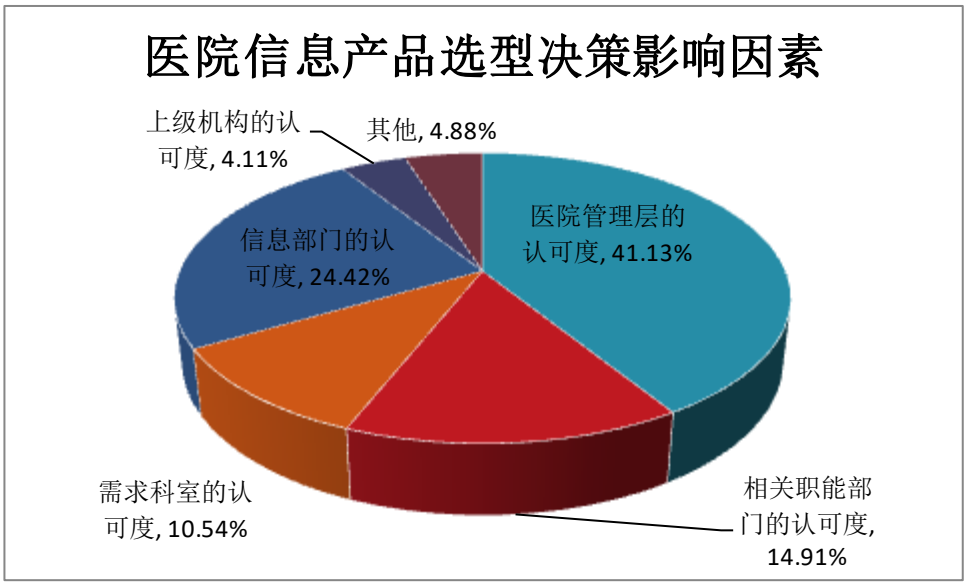




由此可见，大多数医院对于信息安全产品的采购具有强烈的意愿，三甲医院对医疗信息安全解决方案的需求更加明显，医院对医疗信息安全工作的重视在不断提高。

## （十） 信息产品采购选型决策情况

医院信息产品选型一般会由不同的管理层或部门进行认可并决策。此次调查显示，医院管理层的认可度这一因素共有 160

名受访者选择，占比 41.13%；信息部门的认可度这一因素共有 95 名受访者选择，占比 24.42%；相关职能部门的认可度这一因素共有 58 名受访者选择，占比 14.91%。

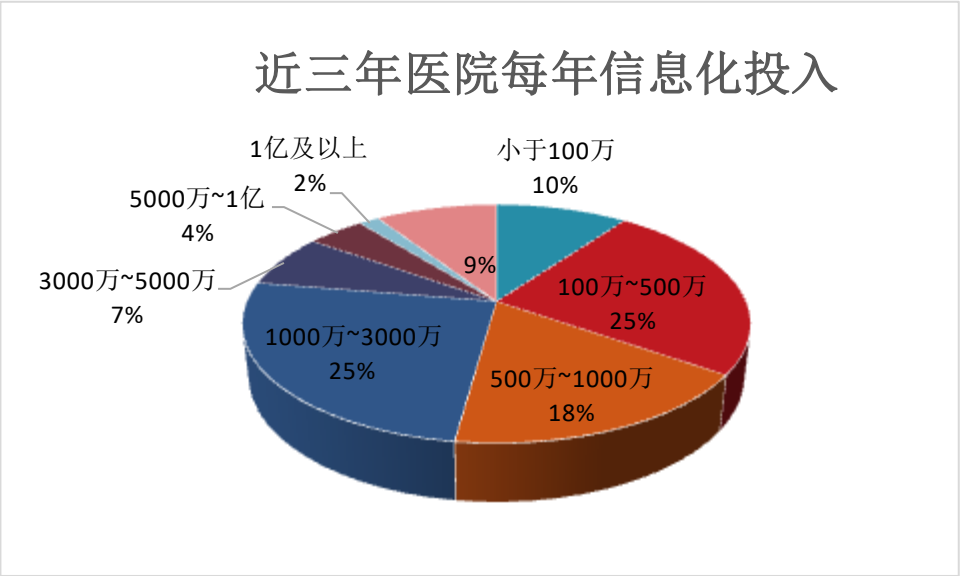



医院信息化建设是经过整体规划、需求分析、应用选型、实施服务、运行维护、评级升级这样一个循环往复不断提升的过程，产品选型是其中非常重要的一个环节。从调查中可发现，医院信息化产品选型是受多重因素影响的，其中最基本的还是要得到医院管理层和信息部门的认可，并满足业务的需求。

## （十一） 医院信息化近三年预期投入情况

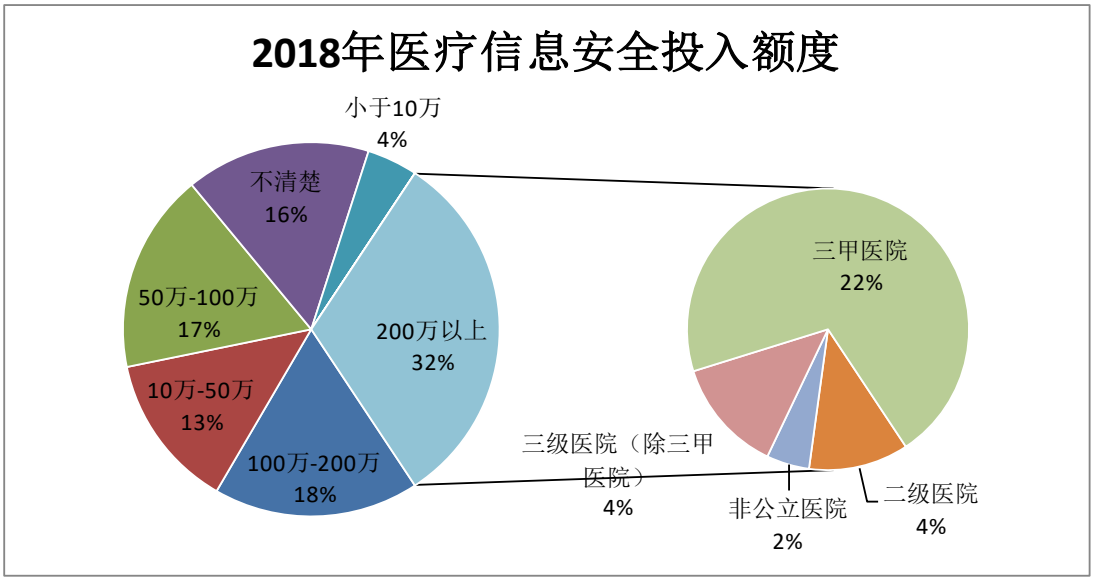
信息系统在医院业务中发挥着日益重要的作用。通过调查医院近三年信息化建设的投入，可发现年投入在 1000 万~3000 万的医院为 99 家，占比 25.45%，其中三甲医院 82 家，占年投入在 1000 万~3000 万的医院比重为 82.82%；年投入在 3000 万~5000 万的医院为 28 家，占比 7.20%；年投入在 5000 万~1

亿的医院为 17 家，占比 4.37%；年投入在 1 亿及以上的医院为 6 家，占比 1.54%。




## （十二） 2018 年建设医疗信息安全投入额度

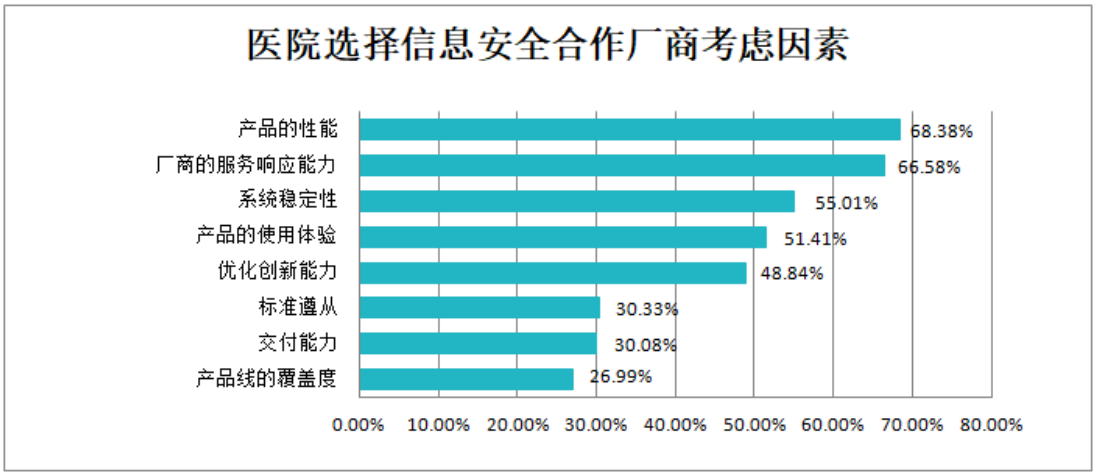
针对 2018 年医疗信息安全的总规划投入的调查显示，年投入小于 10 万的医院数为 17 家，占比 4.5%；年投入在 10 万~50 万的医院数为 53 家，占比 13.62%；年投入在 50 万~100 万的医院数为 67 家，占比 17.22%；年投入在 100 万-200 万的医院数为 69 家，占比 17.74%；年投入 200 万以上的医院数为 122 家，占比 31.36%；不清楚相关投入的医院数为 62 家，占比 15.94%。




通过数据分析可看出，医院对信息安全的投入大部分集中在 200 万以上，其中三甲医院居多。

## （十三） 信息安全合作厂商选择条件因素

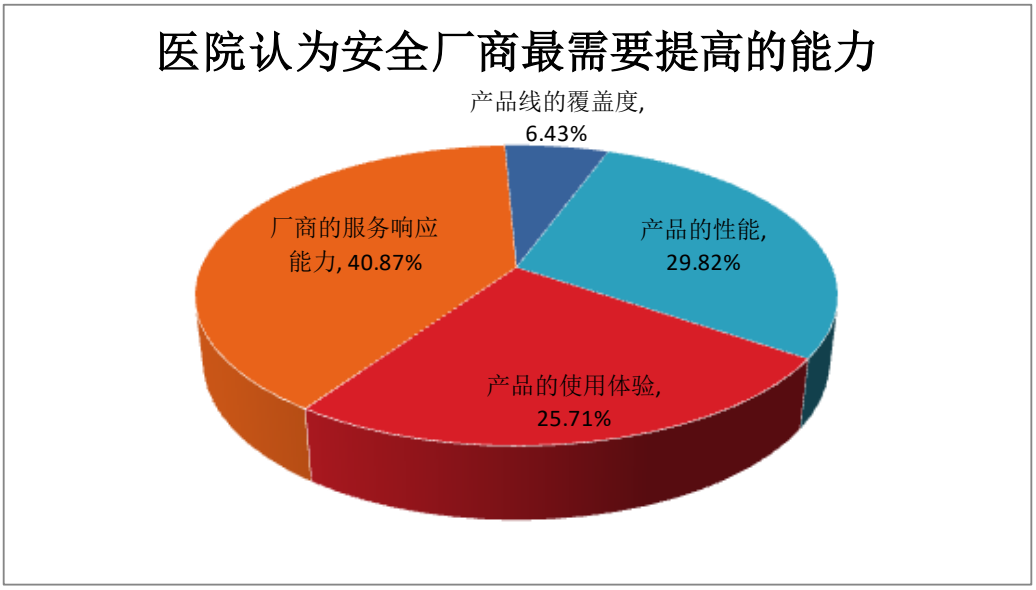
在医院总共 389 位受访者中，在选择已合作的安全厂商中，最看重的能力方面排名过半数的分别是：产品的性能 266 人选择，占比 68.38%；259 人看重厂商的服务响应能力，占比 66.58%；看重系统稳定性的共计 214 人，占比 55.01%；产品的使用体验有 200 人选择，占比 51.41%。



医院在选择信息安全合作伙伴时，看重的是多方面因素，但产品的性能、服务响应能力、提供产品的稳定性和产品的使用体验是首先要考虑的因素。

## （十四） 信息安全产品厂商能力需求情况

在医院总共 389 位受访者中，认为信息安全产品厂商需提高服务响应能力的共计 159 位受访者，占比 40.87%；认为信息安全产品厂商应提高产品线性能的共计 116 位受访者，占比 29.82%；认为信息安全产品厂商应提高产品使用体验的共有 100 位受访者，占比 25.71%。

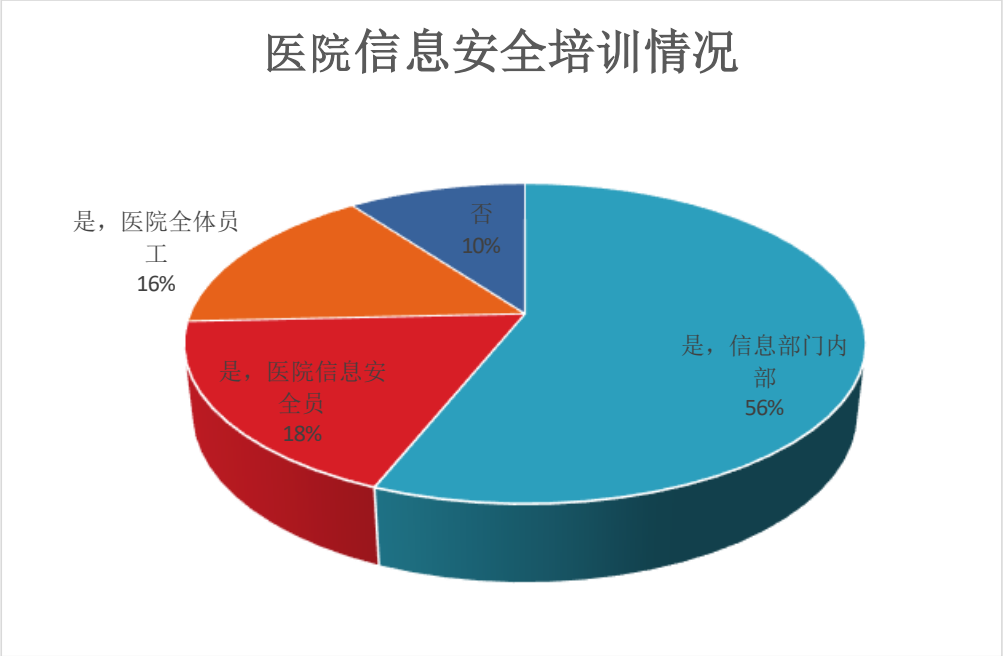



由此可见，医院首要看重信息安全合作伙伴的服务响应能力，并期待提高当前的信息安全产品性能。

## （十五） 信息安全培训情况

此项调查共回收 198 个有效回答，其中 111 位受访者表示

医院会定期在信息部门内部举行网络安全培训，占比 56%；36 位受访者表示医院设置了专门的信息安全员，由他们负责进行网络安全培训，占比 18%；31 位受访者表示医院会对全体员工进行网络安全培训，占比 16%；20 位受访者表示没有相关培训，占比 10%。

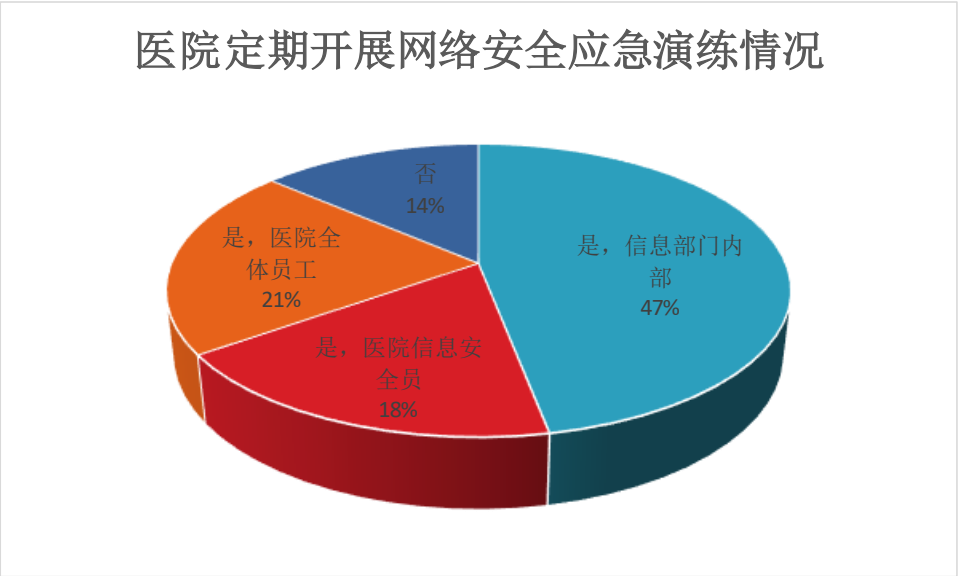



统计数据发现，目前设置专门信息安全员的医院很少，一部分医院也没有进行安全相关的培训，这不利于有效保障医院内信息系统的安全，也不利于提高工作人员的安全意识，信息安全培训频次和意识还亟待增强。

## （十六） 网络安全应急演练情况

此项调查共回收 198 个有效回答，认同信息部门内部组织定期的网络安全应急演练的共计 93 位受访者，占比 47%；选择

医院全体员工负责定期网络安全应急演练的共有 42 位受访者，占比21%;选择医院设立信息安全员的有36位受访者，占比18%;回答医院没有定期网络安全应急演练的有 27 位受访者，占比14%。




由此可见，参与调查的医院定期开展网络安全应急演练的占比不到一半。大部分的演练集中在信息部门内部。

## 四、 现存问题分析

### （一） 不同医院网络安全等级保护工作推进差异较大

调查显示，各单位推进网络安全等级保护工作的力度和进展存在较大差别。12.34%的医院仍未开展科学、合理的系统定级工作，使系统缺乏必要的安全保障措施。即使已实施网络安全等级保护的医疗机构，通过等保三级的系统数量有很大差别，推广的深度和广度差异很大。这就造成医疗信息系统面临的信息安全风险挑战很大，甚至可能导致医疗正常业务受干扰或终

止、个人信息泄露和医疗数据被篡改等严重后果。

从调查结果中可看出，有的医院对网络信息安全不够重视，或对网络信息安全评估的方法有些单一。例如，渗透测试能真实评估信息系统抵御网络入侵的能力，能为信息系统安全防护提供帮助，但是在本次调查中，90.49%的受访医院未做过定期渗透测试，并最终影响信息系统的安全防护能力。各医疗机构需进一步提高对网络安全等级保护工作的认知水平和重视程度，为网络信息安全提供足够的保障措施。

## （二） 网络安全专职人员偏少，需加强培训

从调查中可发现，受访医院设置专门信息安全员的受访者只占 18.19%，仍然有部分受访者表示其所在医院未设信息安全员。医院信息安全工作直接关系到医院业务运作，继而有可能引发社会性群体事件，其重要性不言而喻。从技术角度而言，信息安全工作不可能绝对安全，因此应该在能力范围内减少出错率，降低风险，设置专业的信息安全人员定期进行安全检查、测试、分析等工作十分必要，医疗机构应从网络环境、应用系统、服务器等多方面进行考虑，并制定相应的安全策略。

在本次调查中，10.1%的受访者表示没有受到专业的网络安全培训。因此，网络安全培训需增加并形成常态化，必要时应在全院进行培训，以提高工作人员的专业素养和技能。

### （三） 网络安全投入有待增加

在受访的389家医院中,2018年网络信息安全投入超过200万的医院只占31.36%，有15.94%的医院不清楚投入情况。总体而言，目前医院对网络信息安全的投入仍有待增加。

### （四） 对网络安全和数据安全重视程度需要普及

医院网络安全涉及到日常管理和临床应用的多个领域，一旦遭受恶意攻击，可能导致患者隐私信息的泄露。在大数据时代,医院信息系统内存储了海量数据,一旦发生数据安全问题,会产生非常恶劣的影响。

不过通过本次调查显示，医院当前对网络安全和数据安全的重视仍然不乐观，对安全的重视程度需要普及。

## 五、 相关政策建议

通过本次调查，可以发现医院近年来医疗信息化建设投入逐渐增高，但在网络安全领域的投入仍然偏低。随着云计算、大数据等先进的信息技术在医院应用越来越普遍，患者的健康数据获得了统一管理。但是，这些数据也面临着网络攻击和泄露的风险，不仅严重威胁医院业务系统运行，还将给患者生命健康和财产带来严重威胁。

为推动医院网络信息安全的有序发展，实现强有力的安全防护，提出以下建议：

## （一） 有效化解医院网络信息安全主要矛盾

当前医院网络信息安全的主要矛盾是日益增长的网络信息安全需求与相对落后的安全生产力之间的矛盾。信息安全是医院信息化建设的永恒主题，因此应理解网络安全工作开展的意义与重要性，增强网络信息安全意识，提高其战略地位，同时通过系列技术手段加强安全防范，例如包括网闸、防火墙、数据库审计、网络入侵检测等技术，建立系列安全策略，保障应用系统整体安全，营造一个健康的网络环境。同时，有条件的医院应积极参与等级保护测评工作，切实提高医院信息系统安全保障能力，促进医院信息化工作的健康发展。。

## （二） 医院网络信息安全投入亟待增加

当前医院内几乎所有业务都实现了数字化，同时医院网络结构较为复杂，涉及到多个链接，对网络的稳定性和安全性都提出了很高的要求。因此，医院应高度重视网络安全，加大投入，确保信息系统安全、稳定运行。

## （三） 医院网络信息安全人才亟待培养

网络信息安全人才的培养是国家建设信息安全保障体系和社会信息化健康发展的重要保证。网络信息安全工作需要相关人员具备多项专业知识和技能，网络安全监测数据分析、日志审计分析、网络与安全设备策略配置、漏洞和风险管理、恶意

代码查杀、故障及安全事件应急处置等，否则无法科学、有效地推进网络安全工作开展。

医院可积极鼓励信息化工作人员参加有关网络信息安全课程学习，提高相关人员的素养和专业知识，培养专业的信息安全人才。

### （四） 医院网络信息安全管理能力亟待提升

医院可按照国家网络信息安全相关法律、法规要求，制定并严格落实网络信息安全管理规章制度，建立岗位责任制，落实责任部门和责任人，按照“谁主管谁负责，谁运行谁负责，谁使用谁负责”的原则，切实履行好信息安全保障职责。

同时，医院应加强对网络设备和网络数据安全的保障。网络设备备份主要是将网络中的关键设备和主要设备设置备份。另外，数据备份也是保障数据安全性和可靠性的一项重要措施，可进行多重备份，而且最好有异地数据备份，并对其进行检查，保证数据的有效性和完整性。

网络信息安全责任部门需定期开展网络安全检查，认真分析评估可能的安全风险和威胁，及时发现信息安全存在的问题，研究制定应对措施，堵塞漏洞、消除隐患。

### （五） 医院网络信息安全测评意识亟待加强

测评认证是现代质量认证制度的重要内容，安全测评是国家和社会对信息安全保障体系进行质量监督与技术控制的有效

方式。医院可根据《网络安全法》的相关规定，采用科学方法积极参与信息安全等级保护测评，并根据相关要求了解医院信息系统安全建设实际情况以及存在的安全隐患、管理漏洞，进行整改，进而提升网络信息安全水平，保障网络信息安全。

如今，网络等级保护法规已逐步获得完善，网络安全的地位日趋提升，医院更应该加强对网络安全的投入，进一步完善信息安全框架，提高信息安全管理，以保障关键业务系统安全稳定运行，保障患者生命财产安全，为“2030 健康中国”落地构筑信息安全屏障。

**本次调查得到了亚信安全、腾讯安全的大力支持和协助，在此一并表示感谢。**

**感谢阅读，欢迎指正。**

报告撰写人：杨永燕、李晶晶、朱丽艳、闫懿、刘华

指导专家：王才有、薛万国、朱卫国、郑攀、孟晓阳

CHIMA 秘书处电话：010-65815977，邮箱：sec@chima.org.cn

或关注 CHIMA 公众号进行留言