CSTC中国评测 见证质量 技术白皮书

医疗行业网络安全白皮书（2020 年）

中国软件评测中心·网络空间安全测评工程技术中心

2020 年 3 月

序 言

新年伊始，一场突如其来的公共卫生事件给我国公共卫生应急响应机制带来了挑战，也将医疗行业再一次推上风口浪尖。大数据、云计算、物联网等新技术在医疗行业的应用不断深入，为医疗服务提供了新的技术支持，有效提升医疗服务水平。我国医疗行业信息化建设正加快开展，而网络安全现状不容乐观，面临的网络安全风险也越来越大。

为此，我们组织撰写了《医疗行业网络安全白皮书 2020》，内容聚焦医疗行业网络安全的政策法规、现状及主要问题，并提出加强医疗行业网络安全防护的建议。

本白皮书的撰写人员有刘思思、徐丽娟、路红、李松恬、黄峥、张德馨，在此还要感谢中国软件评测中心品牌宣传推广部刘喜喜、闫晓丽的编辑及排版支持。

限于研究时间和编者能力，部分报告内容难免存在纰漏，不足之处恳请业界同仁批评指正。

中国软件评测中心　唐刚

2020 年 3 月 25 日

版权声明

指导组：黄子河　安　晖　吴志刚　陈渌萍
编写组：唐　刚　刘思思　徐丽娟　路　红
李柁恬　黄　峥　张德馨

目 录

前 言 ..... - 1 -
一、我国高度重视医疗行业网络安全 ..... - 2 -
（一）国家层面密集出台相关政策法规 ..... - 2 -
（二）各地将网络安全作为“互联网+医疗健康”重要内容 ..... - 4 -
二、医疗行业网络安全形势依然严峻 ..... - 5 -
（一）等级保护工作落实情况不佳 ..... - 5 -
（二）医疗行业网络安全风险较高 ..... - 6 -
（三）安全防护水平相对落后 ..... - 7 -
（四）医疗信息泄露事件高发 ..... - 10 -
三、医疗行业网络安全存在的主要问题 ..... - 11 -
（一）身份认证口令不健壮 ..... - 12 -
（二）网络防护架构不完善 ..... - 13 -
（三）数据备份机制不健全 ..... - 15 -
（四）数据加密措施未落实 ..... - 15 -
（五）网络安全管理不到位 ..... - 16 -
四、提高医疗行业网络安全保障能力建议 ..... - 16 -
（一）重视网络安全基础防护 ..... - 17 -
（二）建设安全计算环境 ..... - 20 -
（三）加强医疗数据安全保护 ..... - 22 -
（四）强化网络安全制度管理 ..... - 23 -
五、做好等保 2.0 时代医疗行业网络安全 ..... - 24 -

前 言

近年来，医疗行业信息化得到全面快速发展，互联网、大数据、云计算等新兴技术与传统医疗不断深化融合，促进了医疗服务水平提升。在今年新型冠状病毒肺炎疫情防控期间，许多医院、基层医疗卫生机构、专业公共卫生机构等通过互联网提供在线问诊、智能问药、药品快递到家等服务，减少了接触传染的风险，增强了就医的便捷性，提高了优质医疗资源的利用效率。与此同时，医疗行业面临的网络安全风险也逐渐增多。虽各方高度重视，但我国医疗行业网络安全仍处于工作起步较晚、整体风险较高、防护水平相对落后的局面，网络安全形势不容乐观。

为了保障医疗行业网络安全稳定运行，帮助医疗行业网络运营者做好网络安全保障工作，中国软件评测中心网络空间安全测评工程技术中心（以下简称“中国评测网安中心”）基于近三年医疗行业网络安全的测评经验，总结分析了医疗行业网络安全发展的现状、存在的主要问题，并提出了增强医疗行业网络安全的建议。

一、我国高度重视医疗行业网络安全

（一）国家层面密集出台相关政策法规

医疗行业网络安全是我国网络安全的重要组成部分，受到国家高度重视。随着医疗行业信息网络技术的深入应用和“互联网+医疗健康”的不断推进，党中央、国务院及医疗监管部门陆续出台了一系列信息化安全建设与管理的政策法规，逐步完善医疗行业网络安全体系。

2018 年 4 月，国家卫生健康委发布《关于印发全国医院信息化建设标准与规范（试行）的通知》，对二级及以上医院的数据中心安全、终端安全、网络安全及容灾备份提出要求。2019 年 4 月，国家卫生健康委发布《关于印发全国基层医疗卫生机构信息化建设标准与规范（试行）的通知》，明确了基层医疗卫生机构未来 5-10 年信息化建设的基本内容和要求。其中信息安全部分包括身份认证、桌面终端安全、移动终端安全、计算安全、通信安全、数据防泄露、可信组网、数据备份与恢复、应用容灾、安全运维等 10 个方面。

2018 年 9 月 13 日，国家卫生健康委发布《国家健康医疗大数据标准、安全和服务管理办法（试行）》，明确责任单位应当落实网络安全等级保护制度要求，对健康医疗大数据中心、相关信息系统开展定级、备案、测评等工作。

2018 年 9 月 14 日，国家卫生健康委发布《关于印发互联网诊疗管理办法（试行）等 3 个文件的通知》，管理办法要求医疗机构开展互联网诊疗活动，应当具备满足互联网技术要求的设施、

信息系统、技术人员以及信息安全系统，并实施第三级信息安全等级保护。

2018 年 12 月 21 日，国家卫生健康委办公厅发文《加快推进电子健康卡普及及应用工作的意见》，对重点工作任务进行部署，要求着力加强电子健康卡应用安全建设及管理，对电子健康卡管理服务系统、识读终端设备、应用密码机、互联网医疗健康服务应用软件等依据国家行业标准实行质量及安全检测，强化个人健康信息安全管理，建立相关安全风险动态评估管理机制，同时要求电子健康卡积极采用国密算法和国产自主可控安全技术，确保居民健康信息的安全。

2019 年 12 月，经第十三届全国人民代表大会常务委员会第十五次会议通过，我国颁布卫生健康领域第一部基础性、综合性法律《中华人民共和国基本医疗卫生与健康促进法》，明确国家采取措施推进医疗卫生机构建立健全信息安全制度，保护公民个人健康信息安全，对医疗信息安全制度、保障措施不健全，导致医疗信息泄露和非法损害公民个人健康信息的行为进行处罚。

2020 年 2 月 28 日，国家医疗保障局、国家卫生健康委员会发布《关于推进新冠肺炎疫情防控期间开展“互联网+”医保服务的指导意见》，要求不断提升信息化水平，同步做好互联网医保服务有关数据的网络安全工作，防止数据泄露。

从陆续出台的政策法规可以看出，国家对医疗行业网络安全高度重视，无论从医院、基层医疗机构信息化建设，还是当前发展火热的“互联网+医疗健康”、“医疗大数据”，到一些基本惠民便民的传统医疗信息系统建设，以及国家出台的第一部卫生健康

领域基础性、综合性法律，无不强调落实做好网络安全工作。

（二）各地将网络安全作为“互联网+医疗健康”重要内容

自国务院办公厅发布《关于促进“互联网+医疗健康”发展的意见》以来，各省市纷纷就“互联网+医疗健康”作出行动部署。国家卫生健康委同意批复示范省区建设，各地相继推进互联网与医疗健康融合发展，同时推进信息安全建设。

2018 年 9 月，国家卫生健康委员会与宁夏回族自治区人民政府共同签订共建“互联网+医疗健康”示范区战略协议，宁夏成为我国首个“互联网+医疗健康”示范省区。2019 年 2 月，《宁夏回族自治区“互联网+医疗健康”示范区建设规划（2019-2022 年）》发布，其中就统一安全保障体系作出规划，推进安全防护体系建设，实现信息共享与保护同步发展。到 2022 年，形成全领域、全方位的安全保障体系。

2019 年 12 月 13 日，四川省发布为推进“互联网+医疗健康”示范省建设部署 23 项工作，其中对严格执行信息安全和健康医疗数据保密作出规定，深化国产密码应用，加强关键信息基础设施、数据应用服务的安全防护。严格落实国家网络安全等级保护制度，妥善保管患者信息、用户资料、基因数据等，对泄露、出售、窃取或者以其他非法方式获取个人信息、非法向他人提供个人信息的行为依法依规予以惩处。患者信息等敏感数据应存储在境内，确需向境外提供的，应依照相关规定进行安全评估。

新型冠状病毒肺炎疫情出现后，许多部门、地方和企业积极

运用人工智能、远程医疗、大数据、云计算等技术助力抗击疫情。例如，平安好医生、叮当快药、阿里健康等互联网平台提供了线上问诊模式，部分解决了疫情期间不敢去医院就医的问题。大数据技术帮助政府搜集、发布疫情信息，实现紧缺医疗物资的信息协同与高效配送。医疗信息化在疫情防控中起到了关键支撑作用。

二、医疗行业网络安全形势依然严峻

在医疗行业信息化建设蓬勃发展的同时，其所面临的网络安全风险也逐渐增多。我国医疗行业仍存在等级保护工作落实情况不佳、整体安全风险较高、医疗信息系统的安全防护水平相对落后的问题，医疗行业网络安全形势不容乐观。

（一）等级保护工作落实情况不佳

自 2017 年《中华人民共和国网络安全法》颁布以来，网络运营者落实网络安全等级保护制度成为法律要求，而整个医疗行业的网络安全等级保护工作开展情况一般。例如，中国医院协会信息管理专业委员会（CHIMA）发布的《2017-2018 年度中国医院信息化调查报告》显示，调查的 484 家医院中，仅有 36.16%通过了等级保护测评，明显低于金融、电信、能源等领域。在 CHIMA《2018-2019 年度中国医院信息化调查报告》中，参与调查的 839 家医院中仅有 43.95%通过了等级保护测评，其中三级医院比例明显大于三级以下医院，三级以下医院中 75%未开展过等级保护测评。可以看出医院对网络安全愈发重视，但整体推进态势仍显缓慢。医疗行业亟需加快落实步伐，进一步梳理信息系

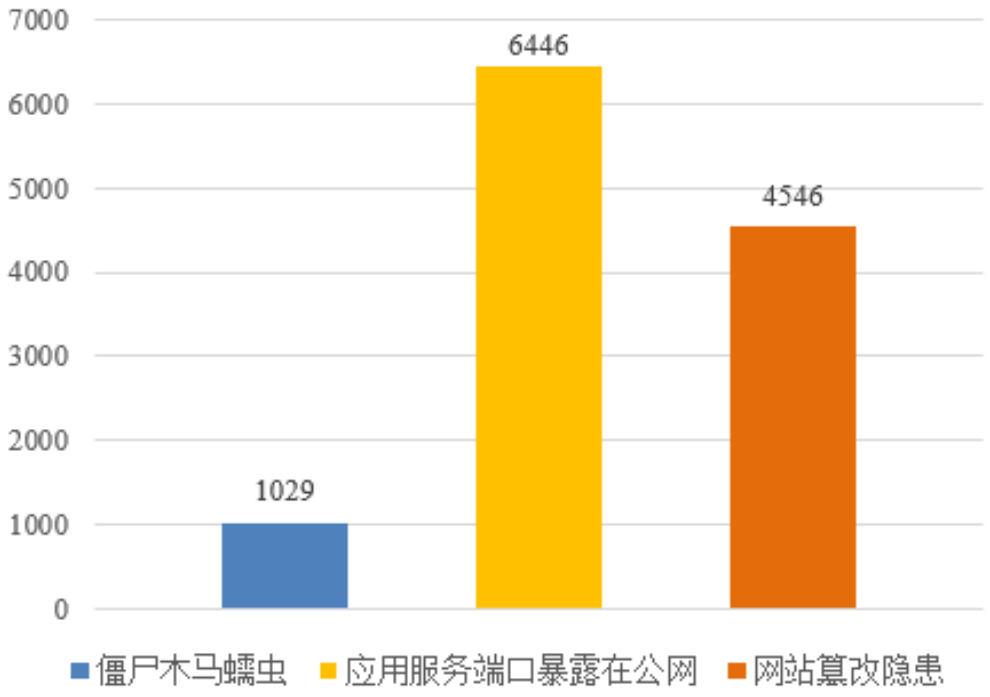
统，开展等级保护测评和系统安全加固工作。

（二）医疗行业网络安全风险较高

1.医疗行业网络安全隐患普遍存在

根据《2019 健康医疗行业观测报告》数据，医疗行业总体处于“较大风险”级别，存在多种网络安全风险及大量可被利用的安全隐患，安全防护能力较弱。报告显示，通过对 15339 家医疗行业相关单位的观测，存在僵尸、木马或蠕虫等恶意程序的单位共计 1029 家，应用服务端口暴露在公共互联网中的单位有 6446 家，4546 家单位网站存在被篡改安全隐患，其中 261 家单位已发生网站被篡改情况。

图 1 三类主要问题涉及的单位数量



（数据来源：《2019 健康医疗行业观测报告》）

通过对观测的 15339 家医疗单位中的网络资产评估，具有脆弱性的有 9523 家，占比 62.14%。由此可见，医疗行业存在可被

利用脆弱性情况普遍，大部分单位没有定期对系统进行安全风险评估，识别资产存在的安全隐患。

随着移动医疗、电子病历系统、AI 医疗等数字化医疗的普及，国内医疗机构遭受恶意攻击的频率更呈上升趋势。2020 年 2 月，在我国正处于新型冠状病毒肺炎抗疫关键时期，印度 APT 黑客组织对我国医疗机构、政府部门展开攻击，以“新冠肺炎”话题为诱饵，引诱受害者执行钓鱼指令。

2.遭受勒索病毒攻击严重

勒索病毒利用加密算法对文件或计算机系统进行恶意加密，使感染者业务中断或数据丢失，只有交付数字货币拿到秘钥才能破解。医疗行业受勒索病毒感染情况严重。根据 2018 年腾讯智慧安全发布的《医疗行业勒索病毒专题报告》显示，在全国三甲医院中，有 247 家医院检出了勒索病毒，以广东、湖北、江苏等地区检出勒索病毒最多。2019 年初，某省几十家互联互通医院同时感染 GlobeImposter3.0 变种勒索病毒而被加密，GlobeImposter 勒索病毒十分偏爱医疗行业，在众多感染 GlobeImposter 勒索病毒的行业中，医疗行业占比约 50%。医疗行业信息系统数据价值高、业务连续性要求强，成为勒索病毒攻击的主要目标，极有可能使医疗单位遭遇巨大经济损失。

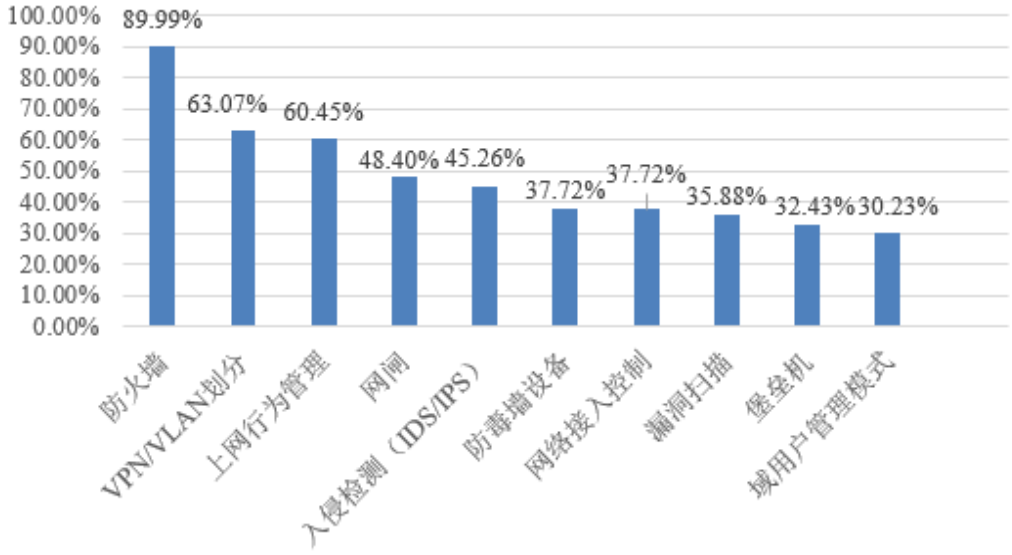
（三）安全防护水平相对落后

1.缺乏必要的网络安全防护设备

根据 CHIMA《2018-2019 年度中国医院信息化状况调查报告》显示，现阶段绝大多数医院仅采用防火墙保障网络安全，对网络

进行 VPN/VLAN 划分和上网行为管理的医院仅过半数。医院对网闸、防入侵、防毒墙等设备的采用率均小于 50%。可见大部分医院都缺乏必要的网络防护设备。

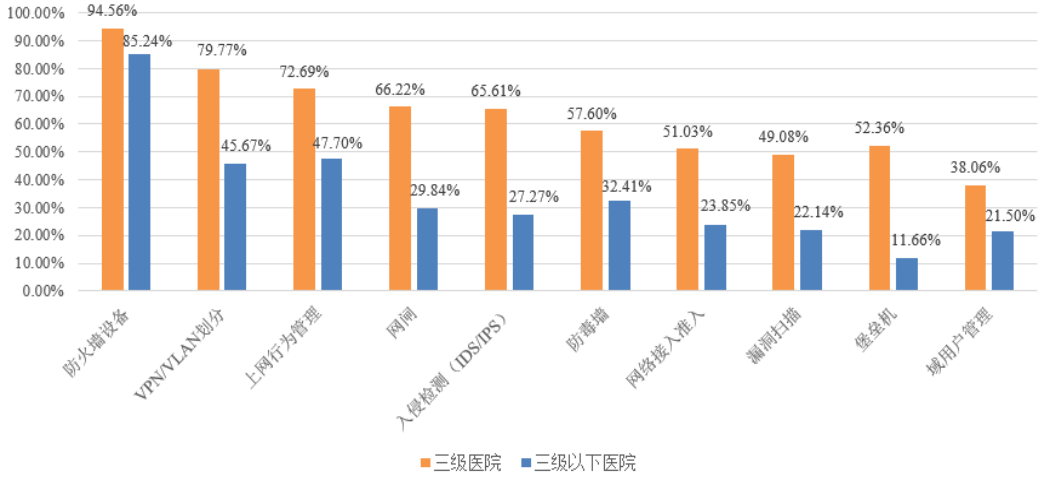
图 2 医院采用的网络安全措施



（数据来源：CHIMA《2018-2019 年度中国医院信息化状况调查报告》）

值得关注的是，三级以下医院只有不到一半采取了 VPN/VLAN 划分、上网行为管理系统，不到 1/3 的医院采用了网闸、入侵检测（IDS/IPS），1/5 的医院采用了网络接入控制、漏洞扫描、域用户管理模式，仅有 1/10 的医院采用了堡垒机进行运维管理。可以看出，三级以下医院在基础网络安全防护方面非常欠缺，网络安全堪忧。

图 3 不同等级医院采用的网络安全措施对比

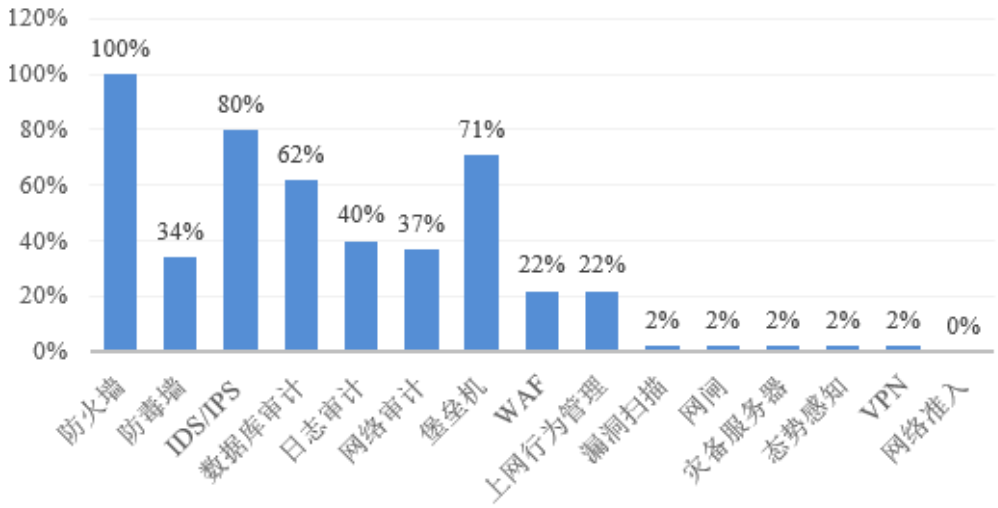


（数据来源：CHIMA《2018-2019 年度中国医院信息化状况调查报告》）

2.缺少必要的系统防护及数据保护措施

医疗信息系统中大部分的服务器操作系统安装了防病毒软件，主要应用服务器采用双机热备或者集群部署，减少了服务器宕机带来的故障，但缺少必要的网络准入机制，对接入网络的终端没有进行 IP 限制，也没有必要的认证机制。中国评测网安中心分析了 35 家开展网络安全等级保护测评的医疗信息系统案例后发现，部署网络准入系统的有 0 家，而在数据保护方面 38%的系统没有数据库审计，只有 2%的单位具有灾备服务器，大部分医疗信息系统没有完善的数据保护机制。

图 4 已通过等级保护的医疗单位采用的网络安全设备



（四）医疗信息泄露事件高发

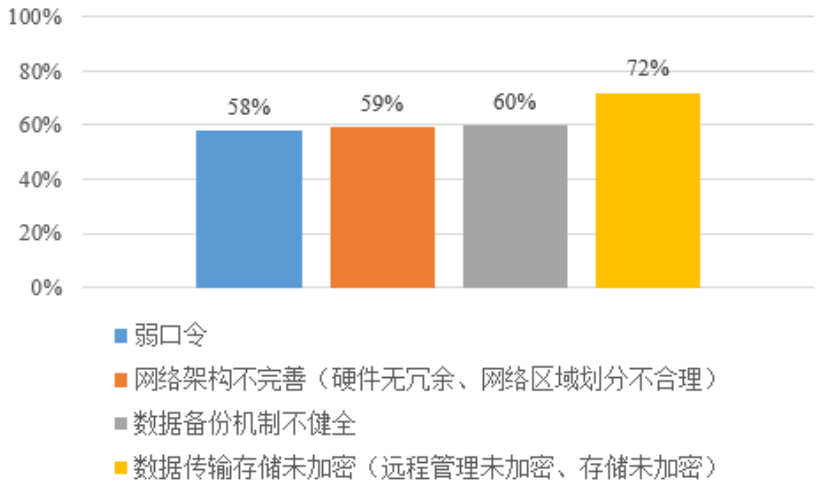
近年来，国内外由于医疗信息系统被入侵而导致的信息泄露事件多次发生。2016 年 7 月，白桦林全国联盟共接到来自 30 多个省份至少有 275 位艾滋病患者的个人信息遭到泄露而导致的诈骗报告。2017 年 10 月，杭州某科技公司在承接某疾病预防控制部门网站信息化建设时，从部门网站上非法下载接种疫苗儿童及其家长个人信息共计 370 余万条，造成了极其恶劣的影响。2019 年，德国一家漏洞分析和管理公司发现，含有大量医疗放射图像的服务器暴露在公共互联网中，其中涉及中国 14 个服务器系统，包含近 28 万条医疗数据，详细记录了患者个人信息及医疗情况，攻击者利用这些数据在暗网中交易获取巨额利润。恶意攻击事件频繁发生，数据泄露成为家常便饭，医疗行业网络安全形势日益严峻。

三、医疗行业网络安全存在的主要问题

随着“互联网+医疗”的迅猛发展和医疗行业信息化建设的持续推进，医疗机构需要关注网络安全防护的信息系统也越来越多，这些系统主要分为两类。第一类是医疗传统信息系统。例如医院信息管理系统 HIS、影像归档和通信系统 PACS、放射科信息管理系统（RIS）、电子病历系统 EMR 等；第二类是利用通信和信息技术实现远程医疗服务类系统。

根据中国评测网安中心对 73 家医疗机构的信息系统进行网络安全测评的结果来看，58%的医疗信息系统存在弱口令问题；59%医疗信息系统存网络防护架构不完善问题，包括网络区域划分不合理、网络链路无冗余等问题。60%的医疗信息系统数据备份机制不健全，包括无异地备份机制、备份策略不合理等问题；72%的医疗信息系统在数据存储和传输过程中未采取加密措施；绝大多数医疗信息系统在管理方面存在监管不力、制度不完善、人员安全意识较弱等问题。

图 5 医疗行业信息系统安全问题占比



（一）身份认证口令不健壮

在网络安全实践中，用户身份认证是信息系统和关键数据保护的第一道防线。当前医疗行业信息系统大多采用安全性较弱的“用户名 ID+口令”的单认证方式，鲜有采用“双因素认证”等强认证方案，医疗信息系统的信息安全程度与登录口令的强度直接相关。信息系统用户多采用易被别人猜测到或易被工具破解的弱口令，使得攻击者甚至无需技术基础就可对目标系统进行攻击。一旦口令被破解，攻击者即可对目标系统进行进一步渗透，给企业和个人带来严重的财产损失。在安全测试过程中主要发现以下几类弱口令情况。

简单口令：口令长度过短，口令仅由简单字符或单词、拼音等组合，非常容易被暴力破解；

默认口令或空口令：很多系统或设备的账号具有默认口令，有的甚至是空口令，不修改默认口令或空口令的情况十分常见，有的系统管理员甚至并不清楚系统里存在默认口令或空口令；

规律性口令：口令具有一定的长度和复杂度，但口令的构造具有规律性，这类口令一般是为了便于记忆而采用了一些简单规律构造而成，如键盘上连续分布的字符序列等。大量规律性口令被收集到口令词典、彩虹表中，极有可能被暴力破解；

社会工程学弱点类口令：为了便于记忆，将个人、单位等信息作为构成口令的部分，如个人姓名拼音、出生日期、单位名称等，攻击者通过社会工程学攻击，搜集特定人员的信息，就很容易攻破此类口令；

固定口令：口令一旦生成，就固定下来，长期不更新，泄露或被攻破的风险越来越大。

（二）网络防护架构不完善

目前“互联网+”的医疗模式发展迅猛，多数采用的结构模式为“医疗机构+平台+患者”。如在线问诊系统中，患者通过身份证号、手机号等信息在平台上进行注册，并将病历等信息通过平台发送医生，医生通过营业执照、资格证书等在平台注册，而后对患者进行问诊。第三方服务平台成为连接患者和医生的关键桥梁，其安全显得尤为重要。若平台的网络架构设计、运行机制的安全性较差，患者及医生的个人信息即存在泄露的风险。

当前医疗服务平台主要存在网络区域划分不合理、设备和链路无冗余、网络安全产品配备不足等安全问题。

1.网络区域划分不合理

网络区域划分方式包括物理划分、功能划分、安全等级划分等。物理划分是指根据物理位置如地理位置不同、所在楼宇不同、所在楼层不同等对网络进行划分。功能划分是指根据业务功能对网络进行划分，如互联网、办公网络、生产网络等。安全等级划分是根据业务数据的安全等级进行划分，不同安全等级的网络区域需要逻辑隔离。

根据医疗行业中业务的种类和信息的重要性，医疗信息系统的网络划分为不同的 VLAN。医疗行业中的 HIS、EMR、PACS、HIP 等系统可能搭建于不同 VLAN 之中，这些系统除了存有各自业务数据外，相互之间还存在数据交互。因此，医疗行业信息系

统网络区域的不合理划分会造成各网络区域内逻辑不清晰、安全策略无法明确、访问控制策略无法有效实施，增大设备被非授权访问进行攻击或破坏的风险，加大了网络安全管理的难度。

2.网络链路无冗余

信息系统是医疗业务运行的关键，必须保证其运行的高可靠性，网络的高可靠性是其基础。目前医疗行业多数信息系统的网络链路存在单点故障问题，如核心交换机、出口路由器、安全设备等关键设备缺少硬件冗余和通信线路冗余。在系统的设备和链路无冗余的情况下，一旦发生电力中断、设备故障、通信线路故障时，系统将无法继续提供服务，形成“信息孤岛”，给医疗行业及患者造成的损失难以估计，极大地降低了系统运行的连续性和可靠性。

3.网络安全产品配备不足

随着“互联网+医疗健康”的迅速发展，HIS、RIS、LIS、CIS、PACS、CPR 等系统的应用逐渐深入整合，为医疗行业的高效、快捷和便民提供了信息化基础。与此同时，为响应国家号召开展的区域医疗协同业务，使得医疗业务网络下沉到区县乡镇，医疗行业的网络不再封闭。而医疗行业现有的网络安全手段已经不足以应对当前内外部的威胁。相关统计显示，大多数医疗信息系统的数据保护措施仅局限于安装杀毒软件和防火墙，而此类保护措施只能防备 21%的安全隐患。网络安全产品的配备不足使得网络攻击者能够轻而易举且不被察觉的入侵医疗信息系统，成为信息泄露、勒索病毒频现的重要原因。

（三）数据备份机制不健全

当前，医疗行业的应用系统繁多，应用环境复杂。HIS 系统、LIS 系统、PACS 和医保等系统的深度融合与广泛应用，产生的数据类型复杂，对数据的增加、更新、修改次数增多。大型医院的数据流量庞大，这些数据一旦遭到破坏或泄露，将严重影响医院的正常运行以及患者的隐私安全，给科研、生产造成损失。

当前医疗行业普遍采用的两种数据备份方式都存在弱点。一是本地存储设备备份，通过硬盘，光盘等数据存储设备存放。该类备份方式不仅占用存放空间，对数据的恢复，查找和分析速度慢，对存放环境要求等级高，且无法支持远程数据容灾。二是本地双服务器备份方式。该类方式容易在其中一套服务器出现未知故障但未宕机时产生主、备服务器争夺控制权的问题，也无法避免双服务器同时发生故障时数据丢失的问题。这两种备份方式都不支持远程数据容灾，无法避免自然灾害等不可抗力因素带来的影响。

（四）数据加密措施未落实

医疗信息包含大量敏感数据，在收集、存储、传输过程中若未实施有效的加密措施，信息将处于极大的泄露风险中。目前医疗行业信息系统中的数据在传输过程中采用 TELNET、HTTP 等协议，无法保证信息在传输过程中被窃听；数据在存储时，采用明文形式、或安全性较低的加密算法进行存储，导致重要数据在存储过程中被攻击者直接盗用的可能性增大，使患者病历等私密信息遭遇泄露，进而可能使医疗机构的业务运营、声誉、经济利益受损，使患者的生命安全和个人信息安全遭到威胁。

（五）网络安全管理不到位

信息使用者和管理者是信息安全管理的主体和关键，对信息使用者及管理者采取规范管理是防止信息泄露的有效方法。当前医疗行业网络安全管理制度不完善，安全管理机构职责不明确，人员网络安全意识薄弱等都是导致信息泄露的安全隐患。

网络安全管理制度包括信息安全管理总体方针策略、各种安全管理活动的制度、人员执行的日常管理操作规程等，是信息系统的建设、开发、运维、升级和改造等各个阶段和环节应遵守的行为规范总体。未制定网络安全管理制度或信息安全管理制度不完善，将无法对信息安全管理过程中的行为进行规范和约束，增加了由于人员操作失误造成信息安全事故的风险。

网络安全管理机构职责不明确将会造成网络安全管理制度得不到有效实施，无法使网络安全管理制度产生相应的效力，增加网络安全事件发生的风险。

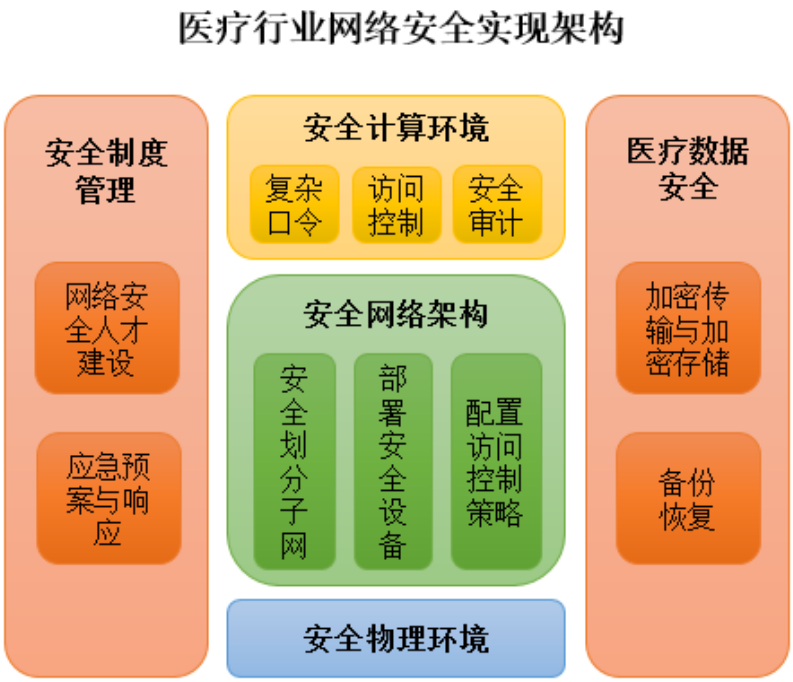
网络安全管理人员安全意识薄弱是造成信息泄露事件的关键原因。如果网络安全管理人员的安全意识和业务能力没有保障，将增大人为操作失误带来的风险。

四、提高医疗行业网络安全保障能力建议

根据医疗行业网络安全现状和保障需求，结合网络安全等级保护基本要求，中国评测网安中心提出了医疗行业网络安全实现架构。该架构分别从安全物理环境、安全网络架构、安全计算环境、安全制度管理和医疗数据安全方面提出了医疗行业网络安全

重点实现内容，其中安全物理环境和安全网络架构是网络安全防护基础，安全计算环境是网络安全防护的重要组成部分，安全制度管理和医疗数据安全工作需覆盖到物理环境、网络架构和计算环境三个层面。基于该实现架构，重点开展以下四个方面工作。

图 6 医疗行业网络安全实现架构



（一）重视网络安全基础防护

1.加强机房安全建设

物理安全是系统安全的基础，保障系统物理安全工作的重点是保护机房安全。如果机房环境遭到物理破坏或非法入侵，那么系统将直接不可使用或者发生数据泄露，这是对系统最简单直接彻底的破坏。这种安全威胁不需要任何技术手段，部署的安全产品都无法发挥作用，所以机房安全建设是最基础的防护措施。

根据中国评测网安中心对医疗行业信息系统的测评经验，在机房安全方面，建议用户关注以下三点。

（1）使用专用的房间建设机房。房间所在的建筑物应具有防风防雨防震能力，机房不能在建筑物的顶层或地下室。

（2）确保机房附近没有水源，防止用水设备故障影响机房设备正常运行。

（3）为机房设置门禁系统并避免闲杂人员访问。

（4）建设灾备机房并实时备份数据。

2.完善安全网络架构

系统网络架构是系统运行的基础，设计安全的网络架构是保护信息系统安全的前提。系统网络架构如果存在安全缺陷，使用再多的安全防护措施都无法修复，并且后期的整改费用昂贵。中国评测网安中心建议从网络规划阶段就重视网络架构安全设计，并关注以下三个方面的内容。

（1）安全划分子网。分出数据存储区、非军事区（DMZ 区）、运维区、办公区等子网，如有必要根据职能不同对办公区做进一步细分。不同子网间部署防火墙进行隔离，避免将重要网段部署在网络边界处，通信线路和关键设备要有硬件冗余。

（2）配置细粒度的访问控制策略。根据中国评测网安中心的测评经验，现在大部分系统的访问控制策略没有设置到协议端口，并且源 IP 地址和目的 IP 地址的范围偏大。建议根据业务理清 IP 间相互访问规则和其间的访问协议，并确保运维区不能直接访问互联网。把访问控制表记录下来，以便后续增加业务需求时与总体访问控制规则保持一致。

（3）使用安全设备提高网络安全防护能力。网络中应部署IDS/IPS、防毒墙、WAF、资源监控系统、垃圾邮件检测系统、上网行为管理系统、堡垒机、日志服务器等安全设备，并定期更新安全设备的规则库和系统版本。

表 1 常见安全设备及生产厂商

安全设备名称	安全功能	常见生产厂商
防火墙	网络隔离，边界防护	华为、H3C、深信服、天融信、山石网科、绿盟科技、网神、启明星辰、网御星云
入侵检测系统	对已知威胁进行监测和报警	启明星辰、绿盟科技、网御星云、华为、安氏领信、交大捷普、天融信、网神
APT 未知威胁发现	对未知威胁进行监测和报警	安恒信息、科来、江民科技、启明星辰
防毒墙	网络防病毒	网神、趋势科技、冠群金辰、瑞星、网御星云、安恒科技、安天、江民科技
WAF	实时监测和阻断 web 应用程序攻击	安恒信息、网神、启明星辰、绿盟科技、天融信、知道创宇、山石科技、安信天行、阿里云、腾讯云
抗 DDoS 产品	防御 DDoS 攻击	绿盟科技、知道创宇、阿里云、腾讯云、网宿科技、网神
网页防篡改	发现网页被篡改事件，恢复正确网页	安全狗、山石科技、安信天行、启明星辰
上网行为管理系统	管理员工在公司用手机/电脑上网的行为	启明星辰、深信服、北信源、网御星云、天融信
垃圾邮件	过滤垃圾邮件	启明星辰、绿盟科技、天融信、冠群金辰、

检测系统		守内安、网际思安、敏讯
主机漏洞扫描	设备漏洞扫描	榕基软件、启明星辰、中科网威、安恒信息、绿盟科技、青藤云安全
Web 漏洞扫描	应用漏洞扫描	安恒信息、绿盟科技、知道创宇、长亭科技、网神、天融信、上海观安
安全管理平台	资源监控	启明星辰、山石科技、天融信
VPN 网关	公网加密通讯	深信服、网神、华为、网御星云、天融信、锐捷网络、渔翁信息、启明星辰

（二）建设安全计算环境

安全计算环境涉及交换机等网络设备、防火墙等安全设备、服务器操作系统、数据库管理系统、中间件和业务系统。在安全计算环境层面，建议重点关注登录口令复杂度和安全审计两个安全控制点。

1.强制使用复杂口令

设备和软件安全的第一道防线是身份鉴别，黑客攻击系统的一般方法首先是猜测或爆破登录口令然后再进行其他破坏操作。身份鉴别是设备和软件安全的重要模块，使用复杂密码，可以有效阻止三分之一以上的网络攻击行为。建议从以下几方面关注用户口令安全。

（1）为设备和软件设置复杂口令并定期更换。按照网络安全等级保护要求，确保口令至少 8 位以上，包含数字、大小写字母、特殊字符中两种或以上，交换机、防火墙、服务器等重要设备的口令在等保要求基础上尽量复杂。

（2）设置企业自己的登录口令，不使用厂商运维人员的口令。同一个厂商的设备可能部署在不同企业，他们的运维人员可能为不同企业设置相同的运维登录口令。这类口令在业内类似于明文存在，应该避免使用这些口令。

（3）避免使用共享账号，不同运维人员不使用同一个账号登录系统。

（4）使用双因素身份鉴别方式。双因素认证的其中一种身份鉴别方式是系统用户所记忆的内容，如口令、身份证号码、PIN码等；另外一种身份鉴别方式是系统用户拥有的实体，如Ukey、动态令牌等。

堡垒机提供定点登录管控和审计功能，在系统设备较多的场景下，用户可以部署堡垒机对系统设备提供统一登录管理。堡垒机将双因素认证、用户权限分配、安全审计功能集中实现，并且能够减少零散管理用户的繁琐。

表 2 堡垒机及生产厂商

设备名称	常见生产厂商
堡垒机	安恒信息、知道创宇、启明星辰、天融信、上海观安

2.注重安全审计

安全审计功能是为了在安全事件发生后可以溯源，以便尽快修复系统，找到事件发生源头，并做好预防和惩戒。一旦发生安全事件，之前做好的审计记录就是修复系统并找到攻击源的重要途径。建议关注以下几个方面。

（1）对重要用户行为进行审计。关注用户登录登出、修改口令、修改用户权限等事件的审计。

（2）保护审计进程。防止审计进程受到未预期的中断。

（3）实时备份审计日志到日志服务器。攻击者攻击系统后会清理攻击痕迹，所以要保护审计进程和审计记录。使用网络审计和数据库审计系统对日常操作行为进行审计。

表 3 安全审计系统及生产厂商

设备名称	常见生产厂商
综合日志审计	安恒信息、知道创宇、启明星辰、天融信、网神、青藤云安全
数据库审计系统	安恒信息、知道创宇、山石科技、启明星辰、天融信、上海观安

（三）加强医疗数据安全保护

医疗行业对数据的保密性和完整性要求都很高。建议从以下三个方面严防数据泄露和篡改事件的发生。

1.加密存储与传输数据

为设备和系统建立普通权限账号，远程访问系统时使用普通用户身份通过 SSH 或 HTTPS 协议。使用加密系统保护医疗数据。

2.加强数据备份与恢复

在医院网络信息化系统中，数据备份尤为关键，这是系统面临安全隐患问题时数据恢复的最佳途径。建议网络安全管理人员根据医院实际情况，从业务需求出发，对各科室的数据进行等级划分，随后按照等级进行数据备份，备份内容可以存储在磁盘或者云平台中。当医院信息系统面临系统数

据不可用时，可通过数据备份将数据尽快恢复，保证业务正常开展。目前医院可以应用 HIS 服务器完成数据存储与保护处理，确保医院所有信息与数据的完整性，为数据恢复奠定基础，确保医院各科室工作正常展开。在系统上线后，实时备份重要数据，定期检查备份数据的有效性，保证备份数据能保存 6 个月以上。

3.注重数据脱敏与分级保护

公众场合或支付场景展示数据时，无论是移动终端还是公示大屏，患者关键信息应该采用脱敏的方式来显示。比如姓名的第二位或第三位、身份证号的部分数字、手机号的部分数字用星号来代替，防止患者数据被其他人员掌握。在数据分级保护方面，不仅对患者病史数据进行分级保护，对医护人员医疗行为的操作权限也应进行分级，需要能够区分在授权情况下医护人员数据调用行为、数据管理员的数据管理行为、应用开发商的软件调试行为，不同的数据访问有相应等级的安全操作。

（四）强化网络安全制度管理

1.完善应急预案与响应机制

建立网络安全应急响应预案，进行预案培训与演练，及时修订应急响应预案。保证发生安全事件时，系统运维人员能有步骤有策略地应对，降低损失。

2.加强网络安全人员管理

建立内部运维管理团队，提高人员专业技能。医院信息化进程中对网络安全人才不可或缺，而现在医院体系里不但缺少网络安全人才，而且缺少计算机专业人才，不能专业地完成信息化建设工作。服务外包形式的前提要有自己的专业人员领导，能够把控外包给第三方公司所存在的安全风险。一是完善岗位设置，在人力资源充分条件下尽量避免网络管理员、安全管理员、安全审计员这三个岗位兼任。二是加强人员培训，根据业务需求为不同人员提供与其岗位对应的技能培训。不但要进行技术人员培训，系统使用者的培训也尤为重要。三是强化人员考核，通过考核督促相关人员主动提高专业技能，并提高培训效果。

五、做好等保 2.0 时代医疗行业网络安全

等保 2.0 时代在等保 1.0 的基础上增加了云计算、大数据、物联网、移动互联的安全合规要求。近年来，云计算、大数据、物联网和移动互联等新兴技术不断与传统医疗业务深化融合，为医疗服务提供便利的同时也引入新的安全风险。

云计算技术帮助实现医疗数据存储和管理，方便区域内医疗机构数据交互共享，使用云计算技术存储和管理这些数据可以降低数据存储成本，提高系统性能和可扩展性。同时，云计算技术的使用也使得医疗数据、医疗信息系统中心化，一旦云平台出现问题，可能导致众多医疗信息系统业务中断、医疗数据丢失，影响医疗活动的正常开展。

大数据技术可以对医疗数据进行专业化分析和再利用，有效进行前瞻性预测及预警。医疗大数据采集、传输、存储及应用大量医疗数据，这些数据具有隐私性强、可利用价值高、来源广泛的特点，常常成为黑客重点攻击目标，存在医疗数据泄露的风险。

物联网技术帮助实现对患者的智能化医疗，主要应用在人体健康数据监测和体内植入设备。例如血糖监测设备、老年人生命体征家庭监控、心脏除颤器、起搏器等。物联网医疗设备也存在信息被监听、截获从而控制设备发起攻击的风险。2017 年，美国 ABBOTT 公司 46.5 万个心脏起搏器因存在安全漏洞而被召回。2019 年美敦力公司收到美国国土安全部的警告，其公司的植入式心脏装置存在被恶意攻击风险。这些物联网医疗设备成为新型的杀人武器。

移动互联网技术应用较多的是移动医疗 APP，这些 APP 深入医患互动中，为医疗信息展示、线上医疗服务提供便捷途径。移动互联网医疗网络安全风险主要体现在数据平台分散化，移动终端难以集中管控，移动数据公网裸奔，容易造成敏感信息泄露等问题。

关注医疗行业网络安全，特别是新技术引入的网络安全风险不可忽视。等保 2.0 从数据保密性和完整性、个人信息保护、通信网络安全、移动应用和移动终端管控等多个方面提出安全要求，保护云计算、大数据、物联网和移动互联等新技术的安全应用，为医疗行业网络安全保驾护航。

网络空间安全测评工程技术中心

地　址：北京市海淀区紫竹院路 66 号赛迪大厦 4 层

传　真：86-10-88559332

手　机：86-17601016287（刘思思）

86-15110214258（张德馨）

邮　箱：liusisi@cstc.org.cn(刘思思)

zhangdx@cstc.org.cn（张德馨）