浅析医院信息管理系统网络安全管理与维护措施

张伟

重庆大学附属三峡医院 404000

【摘 要】随着时代不断进步，信息技术加速发展，医院日常信息管理也逐渐完善，很大程度提升了医院的工作效率。医院想要确保信息系统的安全性，就要保证计算机网络系统工作时能有一个稳定安全状态，医院有必要建立起对系统网络的日常维护工作，不断加强信息管理系统。本文围绕医院信息系统安全管理与维护意义进行简要介绍，以此来解析当今医院信息管理系统所存在的安全管理问题，并针对目前较为典型的问题提出相应对策，提高人员网络安全防范意识，加强中心机房安全管理，强化医院对备份数据的看管，优化网络设施环境，从多方面完善网络安全管理保护，构建较为完备的信息管理机制。

【关键词】医院；信息管理系统；网络安全；维护措施

前言

随着信息时代的到来，互联网成为了广大企业管理模式的新特征，同时也推动了医疗相关的全新改革。医院跟随时代脚步，不再使用传统信息手段，逐渐和云计算、计算机等全新技术相互融合，运用计算机承担起相关医疗信息组成的管理平台，大幅度提高了医院信息的传播速度，有效加快了医疗人员工作效率。信息系统给医院带来便利的同时也伴随着巨大隐患，可能会被别有用心的人侵入数据库，盗取信息等。因此，医院要及时构建起安全防护体系，承担起保护病人隐私的责任。

一、网络安全管理与维护的必要性

当下，大众对医院的服务方面有着较高的期望，为了能够尽快适应社会发展的步伐，多数医院在提升自身管理的过程中，加强了对网络信息系统的运用。互联网信息系统要配合计算机平台进行使用，在其移动互联网、大数据、云计算等科技技术的交融下，可以实现医院管理与信息技术的契合。

根据使用过程来看，网络信息技术给人们带来便利的同时，也存在一些弊端，一方面，在实现医疗人员、药剂、医疗器材等科学部署的同时，能良好顺应社会趋势，大幅度提高了人民幸福指数[1]。另一方面，网络计算机技术存在一定的风险性，在信息系统日常运作中，可能会有外部人员的恶意侵入，这会导致医院内部信息泄露，存在数据丢失或被篡改等问题，极大程度增加了医院对系统数据的管控难度。丢失的信息中含有患者的隐私信息，若属于三甲和高等医院的系统信息中还会存有的重要的医疗手段及其他科研成果，如果这些信息一旦泄露，没有得到安全的保障，势必会引起不轨人群的注意，潜入医院内部系统中，盗取病人的私密信息和医院研究多年的医疗成果，这会影响到医院的科疗发展，给医院的信誉造成严重的打击。科技信息的新时代，要通过网络针对信息系统进行维护，这样才会降低不确定因素的发生，并有效控制信息泄漏，这样会给广大患者带来安全、可靠的医疗服务，满足大众人群的医疗需求。

二、医院信息管理系统存在的问题

随着层出不穷的网络技术被医院灵活运用，在日常工作中信息系统发挥出了至关紧要的作用，就像人类的大脑控制了每一工作环节，若系统出现问题，整个医院就会瘫痪状态[2]。网络就像是人的血管，传输各种医疗信息，如果网络不通畅，就会影响到医疗人员的日常工作，导致信息无法快速传递，影响到整个医院的运作。由此来看，定期检查信息系统，时刻维护网络安全，预防系统出现异常情况，这会影响到医院是否能正常运行。通过“网络信息+医疗”管理下的医院，信息系统在长期的运作过程中会出现诸多问题，若相关医疗人员网络意识薄弱，或操作不熟练，就会导致医院数据的丢失、毁坏等问题。这些问题若不能及时解决，做为信息系统的互联网大脑就会因为数据堵塞无法正常输送，最终导致信息系统不能进行安全运作。

（一）从业人员缺乏网络安全意识

部分从业人员对网络安全意识较为薄弱，上述的从业人员是指网络管理员。医院网络管理人员的信息安全教育欠缺，这在极大程度上对网络信息产生了安全隐患。若是这个问题不能得到有效解决，会导致信息系统陷于危险境地，还会频发各种网络问题。网络安全意识薄弱的体现主要为以下几点：打开计算机浏览网络信息时公开输入密码、没有对电脑进行密码加密、外网连接信息系统、不对计算机进行杀毒预防或遇事离开，导致一些内部机密被外部人员浏览，这些网络安全问题将会严重影响信息系统的正常运行。

（二）中心机房的管理尚不完善

这里的数据中心机房是指海量系统数据储备的关键场所,也是医院信息化的核心区域，其意义重大不言而喻，但数据中心机房往往非常薄弱。然而大部分医院对中心机房的管控比较松懈，尤其是炎热季节，网络设备在工作过程中会持续发出热量，导致中心机房的温度不能得到有效控制，容易引发线路失火等现象。亦或是机房灰尘过多，一些设备在运行的过程中会产生静电吸引附近的灰尘侵入设备，附着在电路芯片上阻断电流，长此以往，会造成电脑短路，影响信息系统的安全运行，对此要制定好相关清洁排表。因此，医院管理层要重视信息系统管理这一问题[3]。

（三）医院数据容易丢失

在医院时常有丢失数据的情况发生，具体原因有以下几种:一是客观原因。在信息系统日常升级或是工作中有存有无法避免的自然灾难，例如天气燥热发生火灾、地震、洪水等，容易造成信息数据的毁坏及丢失，亦或是不法分子对网络入侵进行恶意攻击，导致密码流失，医院核心数据被大量偷去。二是主观因素。比如信息系统相关的工作人员未及时备份数据，从不对计算机进行杀毒处理，设备维护人员工作散漫等。可见，因主客观因素的存在，医院频发数据丢失等现象。

（四）系统补丁版本落后

医院想要保证信息系统的安全运作，需要相关工作人员在日常的信息管控中下载并安装杀毒软件及系统补丁。通过杀毒软件来清除系统漏洞，这样才能降低潜在的病毒风险，要定期更新系统补丁弱化偶然或是来自外界的恶意攻击。但是在日常信息管理中，医务计算机数量较多，管理维护相关工作人员难免会疏忽遗漏，不能保证每一台计算机都更新了杀毒软件和系统补丁，间接导致系统补丁版本过低，不能有效预防病毒漏洞，这会给医院信息系统带来巨大的风险。

（五）信息系统网络安全漏洞较多

随着网络信息技术的高速发展，信息系统的安全也逐步壮大，这是一个不断进步和改进的过程。若是网络防范措施追赶不上信息技术，那么信息也不再安全，就会发生丢失数据等现象。在开发信息系统的过程

中有许多不足之处需要改进，无法做到面面俱到，虽然技术上已经有很大的提升，但是漏洞也会随之出现，医院信息管理人员只能最大化的进行防范，若是在网络信息发生事件之前就已经采取了备份等相关预防措施，就可以最大程度上降低数据流失。然而有很多医院在系统信息防护上，没有做过多的规划和准备，对信息网络的工作认识上存有差距。目前相关医疗人员多数不了解信息安全、制度、流程，没有建立起网络信息安全的体系，信息系统的安全状况漏洞百出。目前的医院只有极少数工作人员对信息系统安全有一定的了解。

三、医院信息管理系统网络安全管理与维护措施

通过上文对医院的信息系统安全防控等相关问题进行了分析，可以发现有很多因素会影响到医院的信息系统，这些网络安全隐患问题很普遍，若不能得到相关管理层的重视，这对正处在“信息+医疗”高度融合及快速发展背景下的医院来说，一但发生意外，就会导致广大患者的个人信息从医院中流出，进而引发一场重大的网络信息安全事件，导致医院不被群众信任的局面。医院要尽快完善和丰富安全制度，同时妥善规划应急事件操作流程等。

（一）提高人员网络安全防范意识

根据前文阐述的当今信息化建设医院与网络信息安全的现状，总结出了医院网络信息安全的主要原因，医院要全面提高信息系统安全，加固医疗人员对网络安全的防范意识。妥善规划医院网络信息安全的主要对策[4]。

首先，医院要加强管理者的网络安全防范意识培训，这样才能更好的带领全体医疗工作人员进行各种网络信息预防管理工作，进一步促进医院整体防范意识。要建立起信息安全制度，采取有效的技术管理措施，加强相关人员的责任感，以此来确保医院信息系统的正常运作，最大化保证病症患者的隐私，维护医院的社会声誉。

其次，灵活建立网络应急的处理制度，若有意外发生也可以及时确反应进行精确的判断，尽量避免突发事件带给医院信息系统运行的不利影响。责任人也要加强日常的安全管理和检查，同时医院信息系统值班人员要注意卫生的打扫，保持地面无灰尘，禁止在机房内吸烟、吃零食、杜绝一切富有安全隐患的行为。并对值班期间的信息系统运营情况做好记录，违反规定者要根据事实情况进行处罚，这样可以最大化确保信息管理制度的规范性[5]。

再次，要贯彻网络信息安全制度的实行度，完善奖励与责任划分机制，有功者要给予丰厚奖励并在整个医院通报并进行表彰，这样可以大幅度提升相关负责人员对网络信息安全工作的积极性，要落实对网络安全管理不当人员进行处罚，情节严重者需要调度岗位或进行开除处理等，这样做的目的是为了把信息系统安全观念树立在每个人心中，可以最大程度保证医护全员在今后的防护工作中落实网络安全责任，以此来保障医院网络安全和广大患者的隐私权益。

（二）加强中心机房安全管理

中心机房是信息系统运作的关键场所，对于环境的要求也是极为严格。中心机房的室内温度要求不得高于25℃，要在30%~70%之间，因此要在室内安装除湿机和空调来保证信息系统日常的运行。其次，要把中心机房布置在安静偏僻的区域，以免人流走动或噪音带动灰尘侵入到线路及芯片之中，并使用两路供电来预防信息系统出现短路等其他意外情况的发生。再次，网络管理人员每天都要对电源、路由器等等进行全方位维修和检查，以此来确保信息系统的正常运作[6]。

（三）强化医院备份数据的管理

首先，医院要明确核心数据的保护等级，建立起核心信息的阅读权限，相关网络防护人员要及时对数据进行备份，避免不法分子对信息系统进行攻击，从而导致核心信息丢失。其次，为了最大程度保障数据安全，医院要使用刻盘的方式进行储存，一旦受到黑客攻击也可及时恢复，以此来保证医院能够正常运行信息系统。再次，医院应在机房设立多个服务器进行备用，当正在工作的机器发生故障或其他原因，也可以使用其他服务器，这样可以做到迅速交接数据，以确保整个医院可以正常工作，不会出现瘫痪等现象。

（四）优化网络设施环境

因为设备要持续运行，所以设备的环境也影响医院网络信息系统安全的一大因素。管理人员在对系统安全防范过程中，要对有可能发生外来因素做出妥善的物理保护，若遭到自然力或人为的恶意破坏也能保证信息系统的安全。从医院的构造来看，总而言之主要保护对象在中心机房以及接口设备，机房是医院的核心信息管理区域，相关设备管理人员应对该房间设置高级密码锁，对机房进行温度控制，避免线路问题引发火灾以确保信息系统的安全问题。日常系统信息管理中，应对核心信息进行多重备份，若出现紧急状况，也可以保证医院信息系统的正常运作。此外要严禁工作人员携带易燃、易爆、易碎、易污染和强磁物品进入计算机房，最大程度上预防外界不确定因素，确保信息系统在运行时的稳定和安全性。

（五）构建网络安全防护系统

对于网络安全的漏洞，可以运用多种安全措施一同进行防护检查。首先，要定期对网络安全进行评估检验，排查出可能威胁到网络安全的漏洞，制定出补修相关的方案，针对重要数据进行严密保护，设定访问权限的等级分类。其次，搭建起危险检测系统阻止非法病毒的侵入，有效隔离各种危险因素，学习并提升信息技术，加强医院对信息数据的保护。最后，要制定好网络信息安全的规定，并严格执行每日杀毒计划，定期升级杀毒软件防止遗漏病毒，从而提高信息系统安全性，达到稳定运行的效果[7]。

总结

医院是一个面相大众的诊治服务单位，通过治疗疾病保护大众的生命安全。随着信息化建设的深入，医院跟随时代的脚步迎合信息化建设，并做出了较好的成绩。但还是有很多不稳定因素的影响，医院信息系统仍有许多方面的威胁。因此要落实医院信息防护管理的相关措施，从而能够全面提高医院的内部信息安全。对此，相关医疗人员要加强网络安全问题的分析，选取对应解决方法进行有效防范，进而提升我国医院网络信息的安全性。

参考文献：

[1]司萧俊.基于医院信息系统的终端安全管理系统研究与设计[J].电子技术与软件工程,2022(19):259-262.

[2]万隆,张洁,李振叶.数据库安全管理与医院信息管理系统的研究[J].科技视界,2021(30):64-65.

[3]殷焕炯.试析网络安全及医院信息系统安全管理研究[J].中国新通信,2021,23(18):115-116.

[4]赵昱.新时期医院信息系统的维护和网络安全管理[J].中国新通信,2021,23(18):128-129.

[5]王君.互联网背景下加强医院计算机信息管理的措施研究[J].智慧健康,2021,7(22):19-21.

[6]于蒋筠.研究医院信息系统的网络安全管理与维护[J].智慧健康,2021,7(22):22-24.

[7]徐钟妍.浅析“互联网+医疗”背景下医院信息系统的网络安全管理问题及解决对策[J].今日财富,2021(09):99-100.