医院信息化建设中计算机网络安全管理与维护

金 扬
北京市海淀区妇幼保健院，北京 100080

[摘要]各医疗机构为了响应国家“互联网+医疗卫生”的规定要求，正在全力建设智能医疗应用系统，完善医疗应用系统基础化建设，对医疗质量持续加强监督和管理，为医疗机构互联网平台提供安全保障。医疗机构可以根据国家相关规定在实体医院的基础上建立网络医院，允许对一些慢性病和常见病进行网上会诊和随访。医院为了给患者提供身体健康管理，可以建立互联网医疗信息平台远程服务。现阶段，医院信息化建设在我们国家已经进入到了一个新进程，二级以上医院基本建成了HIS、PACS等基础信息系统，对于患者服务和医院管理已经初步形成了信息数字化，医院的服务水平得到了有效的提高，也为病人提供了更便捷、更优质的服务。计算机网络技术的不断发展，为医院信息化建设奠定了良好的科技基础。计算机网络技术与医院管理的合理结合，可以使原来复杂的工作逐步人性化、标准化。

[关键词]医院信息化；计算机；网络安全；管理与维护
DOI：10.33142/sca.v4i6.5061 中图分类号：R197.3;TP393.08 文献标识码：A

Management and Maintenance of Computer Network Security in Hospital Information Construction

JIN Yang
Beijing Haidian District Maternal and Child Health Hospital, Beijing, 100080, China

Abstract: In order to respond to the requirements of the state's "Interne + medical and health", medical institutions are building intelligent medical application system to improve the basic construction of medical application system, continuously strengthen supervision and management of medical quality, and provide security for medical institutions' Internet platform. Medical institutions can establish online hospitals on the basis of physical hospitals according to relevant national regulations, allowing online consultation and follow-up of some chronic and common diseases. In order to provide patients with health management, hospitals can establish an internet medical information platform for remote service. At this stage, the construction of hospital informatization has entered a new process in our country. Hospitals above level II have basically built his, PACS and other basic information systems. Information digitization has been preliminarily formed for patient service and hospital management, the service level of the hospital has been effectively improved, and more convenient and better services have been provided for patients. The continuous development of computer network technology has laid a good scientific and technological foundation for hospital information construction. The reasonable combination of computer network technology and hospital management can gradually humanize and standardize the original complex work.

Keywords: hospital informatization; computer; network security; management and maintenance

1 计算机网络安全的内涵

1.1 计算机的物理安全

物理安全是指在信息收集、传输、存储、处理、显示过程中，为保证计算机系统安全可靠运行，保证系统不受人为或自然因素的危害，对计算机系统设备、通信和网络设备造成的损害，存储介质设备和人员采取的分发和使用安全技术措施。物理安全包括环境安全、设备安全和媒体安全。环境安全包括灾害保护和区域保护；设备安全包括设备防盗、设备防破坏、防电磁信息泄漏、防线路截获、防电磁干扰、电源保护等；媒体安全是指媒体数据和媒体本身。为了保证计算机物理安全，对于机房的要求标准也较高，设备的防盗、防破坏和防止电磁信息泄漏是计算机设备安全的主要包括内容。

1.2 计算机存储数据的安全性

计算机安全中最重要的是存储数据的安全。它面临的主要威胁包括计算机病毒、非法访问、计算机电磁辐射、硬件损坏等。计算机硬件本身就是一个辐射到太空的强大脉冲源。例如，它类似于一个频率在数万到数百兆周期之间的小型电台。窃贼可以接收计算机发出的电磁波，在计算机中恢复并获取数据。

1.3 计算机硬件安全

在使用计算机的过程中，对外部环境有一定的要求，即计算机周围的环境应尽可能保持清洁，温湿度适宜，电压稳定，以保证计算机硬件的可靠运行。漏电原理是将计算机产生的电磁信号沿电源线通过电源线传输，并使用专用设备截获和恢复电源线的信号。国际标准化委员会的定义是“为数据处理系统和技术的开发和管理提供安全保护，并保

护计算机硬件、软件和数据免受意外或恶意原因造成的损坏、更改和暴露。”公司内部的服务器、路由器等重要信息设备必须由运营商负责人指派专业人员设立和控制超级用户密码。

1.4 计算机服务安全

计算机服务安全是指在计算机应用中保护和识别计算机用户信息的完整性、真实性和机密性。计算机服务安全是指在计算机应用中保护和识别计算机用户信息的完整性、真实性和机密性。它既能满足计算机用户对信息安全的需求，又能抵御各种可能威胁计算机系统的风险。计算机服务安全主要包括连接安全、机制安全和协议安全。近年来，随着计算机应用的普及，计算机的服务安全越来越受到人们的重视，计算机网络安全技术的应用保证了数据的有效性和信息的安全性[1]。

2 医院信息化建设网络安全维护重要作用

医院信息化建设进行到关键时期，除了信息技术之外，还应用了大数据、云计算等技术，为医院自助付费、自助挂号等功能的实现提供技术支持，也为患者提供了诸多便利，医护人员在信息技术的帮助下，工作效率提升，医院效益与战略发展目标也可以得到预期目标。如果各项信息化项目与面临网络安全问题，不仅会泄露患者及其家属的个人信息，还会阻碍医院信息系统的正常运行。所以，医院信息化建设中的网络安全维护，一方面可以保护所有患者、医护人员的隐私，另一方面有利于推动医院本身的健康发展，使医院网络安全防护制度更加完善，通过信息化建设促进医院建设的进步。

3 医院计算机网络安全管理与维护存在的问题

3.1 计算机安全管理与维护重视程度低

当前阶段，医院还没有着重在对系统网络安全防护和控制的进程中利用现代技术进行信息化建设。想要加速促进发展医院信息化建设，首先必须保证计算机的运行环境必须是安全可靠的。当前，有的医院在创建筹备中对计算机网络安全的重要性不够重视，忽略了对其的定期专业维修护理和日常管理，这就导致计算机系统的运行过程中会出现许多不稳定性。此外，医院在计算机网络安全维护和管理方面投入的人力和资金也尚有不足，有关信息系统的数据存储未做好防范方法，计算机系统缺乏技术组织对其进行专门的定期维护和故障排除，致使计算机系统运转过程中存在不确定因素，从而妨碍了医院建立专门的信息化系统平台。

3.2 信息系统存在的安全隐患

使用计算机的时候，如果没有做好专业的防护系统就会受到病毒威胁，这样会导致不同种类的安全问题。现阶段，医院信息系统建设存在一定的安全隐患。计算机的应用程序在运行过程中的不稳定性，将会影响整个信息系统的安全，这样将会影响医院各项工作数据和患者就诊信息的泄露和丢失。在信息技术日新月异的背景下，医院的计算机安全管理系统没有及时得到升级和更新，导致系统在运行过程中不断受到安全影响，如果不大力度对计算机网络进行安全防范和管理，病毒将会攻击医院系统庞大的数据结构使其出现漏洞，继而严重影响医院信息化系统的安全问题，医院信息化服务水平会因此收到影响，也会降低患者信任度和满意度。

3.3 医院信息化硬件设施不完善

为了实现医院信息化高效有序的运行，必不可少的就是高标准的硬件设备。连接医院和系统终端的重要枢纽就是计算机技术。实现医患信息化共享服务的前提和保证就是先进的计算机硬件设备。由于不够重视，且缺乏人力和资金的支持，有的医院对更换计算机新设施设备方面没有高度重视，使高标准的需求在医院信息系统硬件设施不完善的前提下没有得到满足。在使用过程中，由于设备陈旧，会引起计算机出现死机或卡顿等问题，医务人员和医院的工作成果也会受到影响，同时更加影响了患者对信息共享平台的认可。另外，由于医院工作的特殊性，计算机系统必须 24 小时不停的运转。如果硬件设备的质量不达标，会由于温度过高等原因导致系统出现故障，致使医院就诊和治疗服务不能正常进行。

3.4 网络安全人为管理问题

医院信息化建设过程中，依然有人缺乏对网络安全的正确认知，例如专业负责计算机安全问题处理、网络配置岗位的人员数量较少，有时还会由其他工作岗位人员兼职担任，但实际上不仅专业性不强，网络安全维护的工作经验还比较有限，无法快速解决网络安全问题。如果医院内部网络系统面临安全问题，必须进行人为操作解决，但因网络安全技术人员不足，很难快速对症解决，那么网络安全管理的质量、效率也很难得到提升。另外，医院在网络安全管理制度方面的内容需要完善，网络安全维护职责没有落实到个人，指标约束力度不强，安全维护监督与管理不够扎实，很容易埋下网络安全隐患[2]。

4 提升医院计算机网络安全管理与维护的有效途径

4.1 升级信息管理系统

在进行信息系统的安全管理时，对可以保护信息安全的系统和软件做好升级工作，并对一些无用数据进行销毁处理工作，保障重要数据的安全性。另外，对于访问计算机网络系统的用户，必须应用后台身份保密设置，以便更好的保护访问者的隐私，有效提高各类数据信息安全水准。在密码设置过程中，可选择 KPI 管理方式进行应用，有效加强密钥升级管理；在保护隐私安全和管理数据时，可以将隐私数据进行分割保护。通常情况下可以使用访问权限设置和加密技术进行共同运用，可以提高网络信息安全管理的结果和水准。还应该注重定期进行网络系统安全扫描和程序测

验，保证系统始终处于安全状态运行。

4.2 增强信息加密技术

医院储存的大量患者信息都是在进行医疗工作时获取的，这对医院和患者都非常重要。为了保证这些重要信息的安全，医院需要积极应用信息加密技术。端到端加密或线路加密是计算机应用的加密技术。通过使用上述加密技术，可以对线路中的信息流进行有效加密。对于某些需要保密的线路，利用密钥加密的防护方法是安全可靠的，一般情况下，主要的加密软件通常是利用端口对端口的专用方法，它主要从密文的方向对发送文件的明文进行加密，当信息被有效包封时，它将被传输给目标接收者，关于文件接收者而言，用解锁密钥的方式，将密文转换为明文，可以确保信息资料获取和应用的安全性。

4.3 加强相关软件维护

为了使设置出口避免黑客入侵和黑客攻击，医院可以运用防火墙技术对计算机网络系统的安全领域进行防护，将防火墙有效的设置在网络的入口，可以将网络传输过程中的部分病毒有效的过滤，避免病毒入侵计算机系统和网络。在医院计算机网络安全管理和维护工作中，一般采用身份认证、密码和数字签名等方式进行综合利用，从而保证信息的完整性和安全性。一般情况下，要以指定的用户和网络环境为条件才可以使用密钥有效的解除密码，然后获取原始数据。医院在从对计算机网络信息进行安全角度管理的过程中，应充分结合自身实际情况，根据相关规范不断加强网络信息安全管理。

4.4 提出多元化技术性维护举措

4.4.1 安装杀毒软件

医院信息化建设中的网络安全建设，各个系统软件科学、安全管理非常重要，建议应用现代化检测技术，提高网络安全应用能力。尤其是计算机主机、计算机软件，作为医院内部计算机网络系统运行的重要条件，保证主机高效运行可以避免重大安全事故。医院内部的网络安全技术人员，还必须要对计算机软件运行、设置进行检查，定期更新病毒库，安装杀毒软件，从根源上将计算机主机安全隐患及时排除，以免病毒入侵威胁医院的计算机网络系统运行。如果医院信息化建设面临主机安全隐患，那么可以自动发出预警，技术人员及时解决主机安全问题，修复主机系统之后再投入运行。另外，如果医院使用安全客户端，那么客户端可以自动采集主机发出的安全数据，通过数据库、大数据技术判断信息安全性，也可以起到监督主机运行的效果。

4.4.2 重要数据备份恢复

医院信息系统中涉及诸多重要的数据，例如患者个人信息、就诊信息等，当采集到这些数据之后及时备份，通过复制、储存的方式保证系统内部所有数据安全，一旦计算机、系统软件发生故障，也不会威胁到关键数据信息的完整性与安全性，待计算机与系统恢复运行后再自动备份，还可以避免数据遭到破坏。重要数据备份与恢复，技术人员按照医院信息化建设进度、安全数据保护级别需求，自动选择数据备份种类，对备份文件中的信息全面且系统性地进行安全性保护，避免发生数据丢失与泄露。当前医院信息系统搭建中，数据备份的常用方法是多层次冗余备份，即医院数据的本地、异地、定时刻盘备份，可以全方位保证医院重要数据的安全性与完整性。

4.5 建设网络安全维护管理队伍

现阶段很多医院都非常关注网络安全人才培养，而且会在网络安全维护上投入大量的财力支持。为了壮大网络安全维护人员团队，必须重视网络安全防护、管理人才的引进与培养。信息化建设过程中医院要立足于发展现状，引进综合素质高、专业水平高的网络安全维护人员，在医院内部建设一支专业化团队。关于网络安全维护人员培训工作的实施，需要从医院内部展开，所有人员都可以参加，促使其掌握一定的网络安全维护技能，为医院信息化建设与网络安全维护作出贡献[3]。

5 结束语

综上所述，因大数据技术具有融合性、交互性和开放性等特点，大数据技术的快速发展也出现许多新的计算机技术特性，这对防护计算机网络安全有着非常重要的影响。该怎样适应大数据时代，对计算机网络安全开展进一步的加强和提高，是一个重大的问题，应该引起各领域和各层面的高度重视，不然将给公众、单位乃至全国的信息安全带来严重的损失。因此，大数据时代计算机网络安全有着极端的重要性，应该引起我们的高度重视，尤其要坚持问题导向，运用革新思路和系统思维，解决大数据时代威胁计算机网络安全的重点问题，采取科学的方法和策略,对算机计网络安全要提升防护意识、优化保护技术、创新防范模式、完善抵御机制等多方面加强力度着力解决，推动大数据时代计算机网络安全防范取得更大突破[4]。

[参考文献]

[1]夏文英.探究计算机网络安全技术在网络安全维护中的应用[J].数字技术与应用,2021,39(7):3.
[2]罗永杰.医院信息化建设中计算机网络安全管理与维护[J].数字通信世界,2021(7):10.
[3]詹振坤.医院信息化建设中计算机网络安全管理与维护工作思考[J].无线互联科技,2021,18(10):2.
[4]齐红.大数据时代下计算机网络安全防范的研究[J].中小企业管理与科技,2021(28):3.

作者简介：金扬（1989-）女，汉族，本科学历，毕业于北京城市学院，从事医院信息化管理相关工作。