医院计算机网络通信存在的安全隐患及对策

郝　巍
(长春中医药大学附属医院　130021)

摘要：在信息化时代背景下，社会发展与计算机网络通信有着密切联系，对于医院工作的有序开展也是如此。如今，现代化医院发展的逐步实行，让计算机网络通信技术在建设现代化医院方面具有非常重要的作用及意义，有利于提高医院工作效率，促进医院的远期发展。许多的医院都引进了先进的计算机设备以及相应的网络信息管理系统，并且逐步将传统的医疗服务模式转变为信息化医疗服务，促进建立数字化医院，提高医院工作效率的同时，也能够为患者提供更加优质的医疗服务。但是网络通信技术的应用，可以为医院来带好处的同时，也会存在一些安全隐患，时刻威胁着医院网络通信安全。对此，需要针对医院网络通信的安全隐患进行分析，并且提出及采取针对性的应对策略，保障医院网络通信安全，促进数字化医院发展。

关键词：医院；计算机网络通信；安全隐患；应对策略

随着现代化信息技术的不断发展及优化，网络通信为人们的信息获取提供更多的便利，同时也能够提供更多的信息资源以及更加通畅的交流渠道[1-2]。并且计算机网络信息技术在不断发展的过程中，一些网络通信问题也逐渐被优化处理。因此，计算机网络通信技术对于医疗服务方面的内容也更加丰富，有助于数字化医院建设发展。虽然计算机网络通信技术对于数字化医院发展具有重要作用及意义，但是也不可忽略网络通信带来的安全隐患问题。医院在进行网络安全建设的过程当中，可能会因为设备管理不完善以及技术力量薄弱等问题导致网络安全隐患，对医院计算机网络通信技术的安全应用造成影响。因此，加强医院网络通信安全管理已经成为各个医院开展数字化建设的重点关注问题，也是医院必须面对及解决的重要问题[3-4]。基于此，要想有效解决医院计算机网络通信安全隐患，促进数字化医院建设及发展，需要针对医院计算机网络通信技术应用中存在的安全隐患进行分析，并且采取相应的应对策略，预防及消除安全隐患，保证医院计算机网络通信安全。

一、医院计算机网络通信安全

在现代化网络信息技术的不断发展应用在下，计算机网络通信息技术逐步应用到医疗服务领域当中。在计算机网络通信技术的支撑下，不仅为建设现代化数字医院奠定良好基础，同时也促进数字化医院进步发展。医疗事业作为民生事业领域中的重要内容，而医院则是保证人们健康安全的重要承载机构，医院计算机网络通信技术的应用，对于提高医疗服务质量以及促进医疗事业发展具有重要作用及意义。由于医院承载着人们的健康医疗服务工作，因此医院计算机网络通信系统需要保证持续运转，并且要确保医院计算机网络通信安全。若是医院计算机网络通信安全受损，将会造成难以挽回的损害。鉴于此，保证医院计算机网络通信安全，是保障医院医疗服务有序开展，促进数字化医院发展的关键问题。医院在使用计算机网络通信技术过程中，要不断寻找潜在安全隐患，并且针对可能出现的隐患提出相信的应对策略，并且实施应对措施，以此保证医院计算机网络通信安全，更好的实现数字化医院建设及可持续发展，促进提高医院治疗服务质量。

二、医院计算机网络通信存在的安全隐患分析

2.1 病毒及外部入侵问题

计算机病毒入侵是计算机网络信息系统中的重要问题，若是病毒侵入业务网络系统，将会导致相关机密数据泄露，造成数据丢失，甚至可能会导致系统出现瘫痪情况[5]。由于医院的计算机网络有开放性特点，医院在使用计算机网络通信技术的过程中，容易受到黑客的恶意攻击与病毒入侵，导致内部系统受到损害。若是医院内部计算机网络系统受到损害，将会对医院通信数据造成威胁，并且对患者的生命财产安全造成危害。

2.2 医院数据库信息安全隐患

现如今，人们的自我健康意识提升，促使医院的患者人流量大幅度提升。在现代化时代背景下，信息技术的普及应用，医院对于患者的个人信息资料、医生处方、医院收支等资料信息储存也由传统的纸质档案转变为电子档案。因此，对于医院的数据库安全保护也非常重要。医院数据库安全包括数据保存完整度、有效调用等方面，不仅要保障医院电子档案存储设备的使用安全性，同时也要保证档案使用安全性[6]。常见的数据库安全问题包括资料使用时存储问题，例如存储介质导致的数据丢失，或者是数据资料备份不成功等问题。针对这些数据库安全问题，医院需要采取相应的数据库保护措施，以此保证医院数据库信息资料的完整性，避免出现数据丢失情况，有效保证患者个人信息安全及医院信息安全，促进医院运营有序开展。

2.3 医院计算机网络通信安全管理机制不够完善

医院计算机网络通信技术的使用过程中，虽然实现了信息化技术应用，但是在网络安全管理方面仍然存在一些不足。由于传统医疗服务理念的影响，让医院管理重点提升医疗服务质量的同时，疏忽了对医院网络安全的管理，导致医院计算机网络通信技术应用过程中，容易出现一些安全隐患，对医院网络安全造成一定的影响及危害。医院网络安全管理中出现的完全隐患问题，包括以下几个方面：（1）医院工作人员在使用内网时随意应用移动存储设备（如硬盘光驱以及软驱等），容易导致间接和外网进行数据交换，致使数据泄露以及病毒入侵。（2）医院工作人员在使用网络系统时，疏于保护重要数据及资料等，可造成数据泄露。（3）医院网络通信技术使用过程中，疏于定期检查设施设备，导致医院网络通信系统安全指数降低，随时可能爆发安全问题。

2.4 计算机操作人员的操作不当

通常情况下，医院内部工作人员都将使用医院内部网络系统办公，但是由于部分工作人员的网络安全意识缺乏，并且未按照相应的网络使用规范进行操作，容易导致安全配置出现安全漏洞，从而对医院计算机网络通信系统造成安全威胁。若是医院内部员工使用医院网络系统接入一些存在安全问题的外网，可导致计算机系统受到入侵，致使一些重要信息及数据丢失，引发数据泄露事件，甚至会导致医院内网的重要服务器受到攻击，严重危害医院网络通信安全。

三、医院计算机网络通信安全隐患应对策略

3.1 采取有效措施，防止病毒及外部入侵

为了有效避免出现病毒及外部入侵事件发生，医院在使用计算机网络通信期间，需要采取相应的干预措施，提高医院计算机网络通信安全，避免医院内部数据丢失[7]。医院可以借助专业人员力量，为医院网络系统设置相应的安全屏障，例如设置或者提高防火墙屏障，保护医院内部网络安全。或者是增加一些加密技术以及身份认证技术等，作为医院日常工作中维护网络安全的有效措施。加密技术主要是通过对医院中的一些重要信息数据进行加密处理，防止信息数据在传输过程中被非法篡改或者截取。而身份认证技术作为维护网络安全的有效手段，主要是通过对网络操作人员的身份进行认证识别，以此起到保护网络安全的作用。同时也可以采取对医院信息数据进行权限控制，并且依据不同的职位身份给予相应的访问权限，以此提高医院网络通信安全。

3.2 优化医院信息数据的备份功能

现如今，大多数医院都采取电子技术存储患者资料、医嘱档案等医疗信息资料，因此医院的计算机网络通信系统当中，包含多方面的数据资料。为了有效避免出现数据资料丢失，需要及时对医院数据库中的相关数据资料进备份处理，保障医院数据库的完整性。对此，需要通过采取相应的应对措施，优化医院的数据备份功能及数据恢复功能，确保数据库完整。医院可以通过建立相应的数据存储制度，并且严格要求医院工作人员按照相应的存储制度执行，最大限度保证数据库资料完整[8]。例如在对患者信息进行备份时，需要对所涉及到的重要资料数据进行备份，避免因为硬件故障、病毒入侵等问题导致患者信息丢失。并且医院需要针对一些不可抗力的外界环境因素的影响，设立相应的备份功能，避免因为外界因素的影响，对医院秩序造成影响，并且最大限度的降低数据库损失。医院可以通过相应的技术建立容灾备份功能，借助有关技术力量，在发生地震、火灾、洪灾等不可抗力的灾难时，自动对医院的数据库资料信息进行备份保护，避免出现数据丢失的情况，最大限度的保护数据库安全。

3.3 完善医院计算机网络通信安全管理机制

医院计算机网络通信安全存在的隐患问题，不仅要从技术方面进行解决，还需要从管理方面解决安全隐患问题。因此，医院在解决计算机网络通信安全隐患问题时，对网络技术加强的同时，也需要对医院的网络安全管理机制进一步完善，促进提高医院网络安全，有效保证医院计算机网络通信的正常运行[9]。可以通过根据医院面临的网络隐患问题进行综合分析，制定出适合医院信息化发展，符合网络信息安全法律法规，提高医院网络信息安全的安全管理机制。对医院实行全面性的网络信息安全管理，并且对医院的相关信息安全责任进行合理划分，并且可以设置相应的信息安全管理岗位，在医院的日常运用过程中，加强对医院信息安全监管力度，最大限度的保证医院计算机网络通信安全。除此之外，还可以针对造成医院网络信息安全隐患的人员给予相应的处罚及监管措施，明确网络安全责任。例如在医院网络通信安全管理人员的监督下，定期对医院网络通信安全进行管理，及时发现一些潜在的安全隐患，并且提出相应的网络安全管理措施，促进提高医院的整体网络安全，保证医院日常工作的有序开展。

3.4 强化对医院内部工作人员的网络安全培训

医院运营信息化管理推动，医院内部的网络使用涉及范围较广，包括医院的整体管理、财务管理、医生诊治、护士的护理管理以及药物管理等多方面。因此，为了更好的保证医院计算机网络通信安全，需要对医院内部工作人员卡开展相信的网络安全培训，以此提高工作人员的网络安全意识，促进提高医院网络通信安全[10]。对于医院工作人员的网络安全培训，其培训内容可包括病毒入侵危害讲解、网络安全问题讲解，以及对一些移动存储设备的安全应用问题讲解等，杜绝病毒入侵源头，通过提高工作人员对网络安全问题的认识，促进提高工作人员的网络安全意识，在日常工作中严格按照相应的操作规范使用网络。同时要向工作人员强调使用医院内部网络时，要严格按照相应的操作规范进行网络操作，若有违规，则给予相应的奖惩措施。对于医院内部人员的网络安全培训，需要定期开展，引起工作人员对网络安全的重视度，提高网络安全意识。

3.5 定期维护医院计算机软硬件

医院计算机网络通信技术使用过程中，需要定期对医院计算机然硬件设施设备进行维护，提高医院网络安全性。医院可以通过合作相应的计算机维护技术人员，定期对医院的计算机设备进行维护及升级优化，并且从正规渠道下载相应的软件系统等，同时可以在计算机软盘系统当中设置相应的防病毒入侵措施，以此预防病毒入侵，保证医院网络安全。通过采取定期维护干预措施，有效实现医院计算机网络信息系统的维护及优化处理，避免黑客及病毒利用漏洞对医院网络进行攻击，同时要对医院网络系统漏洞加以全面修复，以此将非法入侵者抵挡在网络系统之外，促进保护医院计算机网络信息安全。

结语

现代化信息技术对于医院而言，为医院现代化发展带来了便利，但是也存一些安全问题。对此医院需要根据实际的发展情况以及网络安全需要，采取相应的网络安全应对措施，加强对医院网络信息安全的防护，促进医院现代化发展，同时也为患者提供更加优质的医疗服务。

参考文献：

[1]马啸天. 数字化医院计算机信息网络系统安全及对策研究[J]. 通讯世界, 2021,028(007)59-60.

[2]龙智勇陈姣阳赣萍邓丽君丁长松. 医院信息化建设网络安全与防护问题研究[J]. 医学教育管理, 2021, 007(006):675-679.

[3]王昊. 数字化医院计算机信息网络系统安全及对策研究[J]. 电脑知识与技术:学术版, 2021,017(012):64-68.

[4]唐和秀. 医院信息化建设中计算机网络安全管理与维护[J]. 科学与信息化, 2022(2):174-176.

[5]陈柯. 医院计算机网络信息系统面临的安全问题及防范对策[J]. 信息记录材料, 2021, 22(7):47-48.

[6]郭放. 数字化医院计算机信息网络系统安全及对策研究[J]. 移动信息, 2021(004):1-2.

[7]吴渊洲. 新时期医院信息化建设存在的问题及改进对策探析[J]. 科学与信息化, 2021, 000(018):134-135.

[8]邵琰. 医院计算机网络通信存在的安全隐患及对策[J]. 中国新通信, 2022, 24(16):20-22.

[9]何金新. 浅谈医院信息化建设中计算机网络安全的管理与维护[J]. 科学与信息化, 2021(008):131-131.

[10]唐和秀. 医院信息化建设中计算机网络安全管理与维护[J]. 百科论坛电子杂志, 2022(2):174-176.