医院信息安全：挑战与策略

姚峰

如东县人民医院

摘　要：随着医院信息系统的发展和电子健康记录的广泛应用，医院信息安全面临着日益严峻的挑战。保护患者和医疗保健信息的安全性对于医院及其他医疗机构至关重要。本论文旨在探讨医院信息安全所面临的挑战，并提出相关策略和措施以应对这些挑战。

关键词：医院信息安全；挑战；策略；措施

【DOI】10.12252/j.issn.2096-627X.2023.10.105

在现代医疗环境中，医院信息系统扮演着关键的角色，它们使医院能够高效管理患者数据、提供优质医疗服务并支持决策制定。然而，随着医疗技术的进步和电子健康记录的广泛应用，医院信息系统面临着日益严峻的安全挑战。医院信息安全是指保护患者和医疗保健信息免受未经授权的访问、使用、披露、修改或破坏的实践。医院存储着大量敏感的个人健康信息，如病历、诊断结果、药物处方等。这些信息对于患者的隐私和医院的声誉至关重要，因此必须采取适当的措施来保护其安全。

一、保障医院信息安全的重要性

（一）患者隐私保护

患者隐私保护是保障医院信息安全的重要方面。医院存储了大量患者的个人信息和病历资料，其中包含有身份证号码、住址、联系方式等基本信息，还有病情描述、检查报告、用药记录等较为敏感的隐私内容。这些信息一旦泄漏，可能会直接或间接导致患者个人信息被他人获知甚至被非法使用，使患者隐私权被严重侵犯。例如，患者的手机号码、身份证号码等一旦被盗用，可能引发电信诈骗或其他身份盗窃事件，给患者个人和财产安全造成损害。因此，医院有义务妥善保管患者信息，制定严格的信息安全措施，杜绝未经授权的信息泄漏，从源头上保护患者的信息隐私，维护患者的合法权益。

（二）医疗质量保障

保障医院信息安全对医疗质量至关重要。医院信息系统存储了患者的病历档案、医疗画像、检验报告等关键信息，这些信息与医疗质量和患者健康息息相关。如果医院信息系统遭到攻击，导致医疗信息被篡改或丢失，医生和护士在诊疗过程中就可能获取错误信息，做出错误判断，这势必影响医疗质量和患者健康。更严重的是，关键系统如药房管理、手术室调度等一旦瘫痪，会直接危及患者的生命。近年来，全球多起医疗信息系统被黑客攻击导致医疗服务中断的事件，警示我们必须重视医院信息安全。充分认识到医院信息系统安全对保证医疗质量、患者权益乃至生命安全的重要性，是促使医院加强信息安全管理，预防信息安全事故的重要驱动因素。

（三）防止医疗诈骗和数据篡改

防止医疗诈骗和数据篡改是保障医院信息安全的重要环节。医疗诈骗是指利用医疗信息系统漏洞或非法手段获取医疗资源、虚报医疗费用等行为，严重损害医疗资源的合理分配和医疗秩序的正常运行。若医院信息系统存在安全漏洞，黑客可以伪造病历数据申请不必要的检查和用药，浪费医疗资源；也可能以病人身份多次重复就诊充医保，进行重复报账欺诈。数据篡改可能导致病历数据的错误或丢失，严重影响医疗决策和治疗效果。例如黑客入侵病历系统，篡改患者的用药或手术记录，可能导致医生诊断或治疗失误。因此，医院必须采取必要措施保护信息系统安全，从源头预防医疗诈骗和数据篡改的发生，维护医疗秩序和患者权益。

二、医院信息安全的挑战

（一）网络攻击和数据泄漏

医院信息系统经常成为网络攻击的目标，导致医院面临数据泄漏的严重风险。随着网络犯罪活动的不断升级，医院所面对的网络攻击类型日趋复杂，既包括勒索软件、钓鱼邮件、分布式拒绝服务攻击等方式，也包括通过利用系统和软件漏洞进行的有目标性的入侵行为。这些攻击可能导致病历、诊断报告、医疗图像等敏感数据被非法获取；也可能造成医院信息系统瘫痪，影响医院的日常运转。近年来，不少医院都遭遇过不同程度的

数据泄漏事件，给患者的隐私安全和医院的声誉造成了重大损失。随着医疗信息化水平的提高，以及物联网、云计算等新技术在医疗系统中的运用，医院信息系统面临的网络攻击威胁也在不断增多。医院亟须采取有效的网络防御措施，建立完善的风险评估与危机应对机制，以保护数据安全、维护医疗服务的连续性。

（二）内部威胁

医院内部威胁主要来源于医院内部员工的不当行为或恶意行为。员工由于疏忽大意或者系统操作不当，可能会导致重要数据被泄漏或遭到破坏。例如，员工忘记锁屏就离开办公室，使得他人可以进入系统，窃取患者隐私信息。员工可能错误删除或者篡改重要的医疗记录，给后续的诊断治疗带来困难。一些员工可能存在恶意行为，如出于经济目的刻意泄漏患者信息，或者入侵系统窃取数据进行敲诈。也有极少数员工受外部势力利用，作为内应在系统内进行破坏或植入木马病毒。由于医院内部各系统相互连接，一个环节的疏漏都可能导致整个系统遭到破坏。

（三）移动设备和远程访问

随着移动和远程工作形式的兴起，医疗保健专业人员越来越多地通过移动设备来访问医院信息系统和电子病历，以及进行远程病人监测和远程医疗咨询。这无疑为医护人员提供了更大的工作灵活性，但也增加了医院信息安全的风险。首先，移动设备如手机和平板电脑更易遭受黑客攻击和恶意软件感染，导致病历数据和用户认证信息被非法获取。其次，员工可能会通过不安全的公共WiFi网络来进行远程访问，这些网络的安全性得不到保证。此外，远程访问医院信息系统也增加了医院网络的攻击面。如果远程连接没有得到充分验证和加密，很容易为黑客提供入侵医院内部网络的机会。最后，医护人员外出使用移动设备的情况也增加了设备遗失或被盗窃的风险，这同样会导致敏感数据外泄。

（四）物联网的应用

物联网技术在医疗领域的应用日渐广泛，对提高医疗质量和效率产生重要影响，但也给医院信息安全带来新的挑战。物联网应用使得大量医疗设备和系统相互连接并与网络相连，形成了一个庞大的医疗物联网系统。这些连接的医疗设备包括监测设备、诊断设备、给药系统等。物联网的应用无疑提高了医疗数据的采集、传输和分析能力，使医务人员可以远程监测患者状况。但是连接数量巨大的医疗物联网也扩大了医院网络的攻击面。入侵者可以通过设备的漏洞入侵整个网络，造成更大范围的混乱。此外，大量连接的医疗设备本身存在安全漏洞，如默认密码、系统漏洞、未及时更新补丁等，这些漏洞都可能被黑客利用，危害医院网络安全。

（五）新兴技术的安全挑战

医疗行业近年来积极采用新兴技术，以提升工作效率、改善患者体验。但新技术也带来了新的安全挑战。具体来说，云计算通过网络访问共享的计算资源，使医院可以灵活获取所需计算能力，降低IT成本。但是公共云的安全性难以保证，可能导致患者数据在云端被恶意攻击者获取。人工智能尤其是深度学习在医学影像分析等方面展现巨大应用潜力，但可能因训练数据偏差或算法缺陷而产生错误结果，影响诊疗决策。区块链的去中心化账本为医疗数据管理提供了新的选择，但公有链的开放性与医疗数据的机密性存在矛盾。其他新兴技术如5G、自动驾驶、虚拟现实、3D打印等在医疗领域的应用也需要考虑潜在的安全风险。

三、医院信息安全策略与措施

（一）风险评估与管理

医院应建立规范的信息安全风险评估与管理体系。首先，医院可以成立信息安全管理小组，专门负责对医院信息系统的风险进行评估。评估可以采取定量或定性的方法，识别医院网络、数据资产、系统组件等方面的漏洞和威胁，评定可能造成的影响程度与发生概率，计算出风险值。其次，医院应建立信息资产分类目录，将资产按照重要程度进行分类，重点关注高危资产。另外，评估还要考虑合规要求，识别不符合规则的地方。在评估的基础上，医院可以制定风险控制措施，针对高风险方面采取严格管控，中低风险方面实施常规控制，将风险控制在可以接受的水平。最后，医院要定期审查风险评估结果，跟踪风险变化趋势，对风险控制措施进行持续改进，以保证医院信息安全风险在可控的水平之内。

（二）强化访问控制

医院应当建立强大的访问控制系统，对用户的身份进行认证，严格授权不同级别的访问权限。具体措施包括：实施多因素认证，不仅依据密码，还需要其他身份验证因素，如指纹、声纹等生物特征，或动态验证码等。对重要系统实施双因素或多因素认证，增强安全性。建立细致的角色访问控制模型，不同角色及岗位的员工只授予对应工作所需的最低权限，避免出现因为权

限过大带来的安全隐患。定期审计用户的访问权限，删除及时收回离职人员的权限。对访问系统进行日志审计，监控异常访问行为。重点系统和应用采用单独密码保护，避免因泄漏或被盗用的共享密码给系统带来风险。利用网络访问控制系统进行细粒度的访问控制，对目标IP、时间段等进行控制。采用数据访问控制系统保护敏感数据，对数据实施访问策略。

（三）加密敏感数据

医院可以对敏感数据的存储和传输过程都采取加密措施。对于数据存储，数据库和文件服务器等要部署加密工具，加密存储中的所有敏感数据。常用的加密算法有DES、3DES、AES等对称加密算法。数据传输方面，医院内部网络的通信也应该加密，避免内部网络抓包获取明文数据。与外部系统和设备的连接必须使用安全的数据传输协议，如SSL/TLS。同时，数据共享和报告传输也需要加密。移动设备和远程访问必须要求强制加密。另外，静态数据的加密同样重要。USB设备、笔记本电脑、打印纸质报告等都要规定必须加密然后才能携带使用。加密手段的使用需要政策和规范的支持。医院可以建立数据分类指南，规定不同级别敏感数据必须采取的加密方式。关键数据要求用信任度更高的算法和更长的密钥。不同的数据可以采用不同的密钥或证书，这样即使某一密钥泄漏也不会影响全部数据。

（四）员工培训与意识

医院应当高度重视员工在信息安全中的作用，通过培训和意识培养来提高员工的信息安全意识和能力。首先，医院可以制定信息安全培训计划，要求各部门新入职和在职员工定期参加信息安全培训，培训内容可以涵盖信息安全政策、规章制度、操作规范等，使员工全面了解医院的信息安全要求。同时，针对不同岗位设置不同的专项培训，例如对经常接触敏感信息的医生和护士开展病历数据保护培训，对系统管理员开展网络安全和访问控制培训，针对性强的培训能更好地提升员工的信息安全技能。其次，培训形式上可以采用讲课、案例分析、模拟演练等多种手段，增加培训趣味性和参与度。再者，培训后可以设置考核来检验培训效果，同时将考核结果与员工的职务晋升和绩效挂钩，形成激励机制。最后，除了培训以外，还需要采取多种措施培养员工的安全意识和责任感，例如签订信息安全责任书，开展警示性的宣传教育，举办信息安全知识竞赛，定期进行信息安全评估等，使员工时刻保持警惕并自觉遵守各项信息安全规定。

（五）审计与监控

医院应定期进行信息系统的安全审计和监控，以检测异常活动和识别潜在的安全威胁。医院可以建立专门的信息安全审计部门，由安全专家组成。该部门应对医院网络基础设施、关键信息系统、网络活动等进行全面的安全检查。审计的方法可以包括尝试入侵医院网络来检测漏洞，检查系统日志来分析异常活动，对比网络流量数据来发现潜在的威胁等。医院也应聘请外部的信息安全公司进行周期性的渗透测试和安全审计，提供第三方的专业意见。医院应当部署入侵检测系统、安全信息和事件管理系统等工具，对网络流量、系统调用日志、数据库访问日志进行7*24小时不间断的实时监控和分析。这些系统可以通过分析大数据，检测已知攻击模式的异常信号，发现潜在的威胁，并及时做出响应。当监控系统发现可疑活动时，应立即通知安全团队进行进一步的调查和处理。重要系统和业务应用的日志数据要保存足够长的时间，以备审计之需。日志数据应定期归档，并且有加密和访问控制措施。日志分析可以发现员工的非法访问或异常操作，识别可能的内部威胁。医院应建立信息系统漏洞管理流程。及时对操作系统、数据库软件、网络设备固件等进行补丁更新，降低已知漏洞被利用的风险。对新发现的零日漏洞也要第一时间评估风险并采取应对措施。

结束语

综上所述，医院信息安全面临着日益严峻的内外部威胁，关系到医疗质量、患者隐私以及医院声誉。医院必须认识到信息安全的重要性，建立全面的安全管理体系，采取有效的技术、管理、培训等综合措施，持续开展风险评估，及时应对各种新出现的威胁，以此提高医院信息系统的安全性和可信度。只有不断加强信息安全建设，医院才能确保医疗服务的连续性和质量，维护良好的社会形象和公众信任度。

参考文献

[1]赵敏，叶建平.医院信息安全风险评估与防范对策研究[J].中国卫生信息管理杂志，2023，20（05）：683-688.

[2]王丹，彭清泉.基于物联网的医院医生隐私信息安全存储控制系统[J].自动化技术与应用，2023，42（09）：119-122.