探析医院电子信息档案管理的风险控制

张　鑫

（鄄城县中医医院，山东　菏泽　274600）

摘　要：随着医院信息化建设的不断推进，电子信息档案管理已成为医院信息化建设的重要组成部分。目前，国内许多医院都已经实现了电子信息档案管理。电子信息档案管理具有信息共享、可追溯、安全性高等优势，可以方便医生、护士、患者等多方共享医疗信息，提高医疗服务的效率和质量。但电子信息档案管理地风险系数也在不断增加，一旦被黑客攻击或者管理不善，就可能导致患者的隐私信息泄露或篡改，给患者带来巨大的困扰和损失。本文通过分析医院电子信息档案管理的现状和存在的风险，探讨如何进行风险控制，以保障医院电子信息档案管理的安全性和可靠性。

关键词：医院电子信息档案　风险控制　管理措施

DOI：10.12319/j.issn.2096-1200.2023.14.16

一、引言

近年来，随着信息技术的不断发展，医院电子信息档案管理已成为医院信息化建设的重要组成部分。相比传统的纸质档案管理，电子信息档案管理具有许多优势，因此得到了越来越多医院的认可和推广。然而，电子信息档案管理也存在一些风险，如信息泄露、数据篡改、存储容量不足等问题，这些风险可能会对医院信息化建设带来不良影响，因此必须采取一定措施进行风险控制。

二、电子信息档案的特点

（一）可复制性

电子信息档案的复制具有高精度和高效率的特点。与传统纸质档案不同，复制电子信息档案不会像复印或扫描纸质档案那样出现失真或变形的情况。在复制电子信息档案时，只需要进行文件的拷贝和粘贴，就可以得到与原始文件完全一致的复制品，保证档案信息的完整性和准确性。此外，电子信息档案可以在较短的时间内进行复制，且复制的数量没有限制，具有高效率的优势。医院管理者也可以通过复制电子信息档案来制定医院管理方案和策略，加强医院信息化建设和管理水平。

（二）易传输性

电子信息档案具有易传输性，使得不同医疗机构之间的信息共享更加便捷和高效。例如，通过电子信息档案系统，医院之间可以快速传输患者的病历、检查报告、医嘱等信息，方便医生对患者进行诊疗。此外，电子信息档案的易传输性还可以加速卫生部门之间的信息交流，实现健康信息共享，提高卫生服务的效率和质量。同时，电子信息档案还可以便于患者随时随地查阅自己的健康档案信息，了解自己的健康状况和治疗情况。总之，电子信息档案的易传输性为医疗信息共享和卫生服务提供了更加便捷的途径[1]。

（三）易读取性

电子信息档案的数字化存储方式使得信息的查找、管理更加高效便捷。通过电子信息档案系统，用户可以通过电子设备对档案进行快速检索、浏览、打印等操作。同时，电子信息档案还可以进行全文检索、自动分类、智能推荐等功能，帮助用户更加快速、准确地找到所需信息。此外，电子信息档案可以进行批量导入、导出，以及对档案进行备份和恢复，使得档案的保护和传递更加方便、快捷。电子信息档案还可以进行多维度的数据分析和统计，帮助医院更好地了解医疗业务的情况，提高管理效率，优化医院的运营管理。总之，电子信息档案的数字化形式为档案的使用、管理、保护、传递提供了更加便捷、高效、安全的方式。

（四）易损坏性

由于电子信息档案是以电子形式存储，因此其易损坏性也是不可忽视的。在电子信息档案的存储过程中，可能会受到多种因素的影响，比如电磁辐射、病毒、黑客攻击、操作错误等。电磁辐射可能会导致电子设备损坏，进而导致档案信息的丢失或损坏；病毒、黑客攻击会导致电子信息档案容易受到的威胁，如果安全措施不到位，就有可能使信息泄露或篡改[2]。

（五）易保密性

通常来说，电子信息档案可以采用密码和加密两种安全措施。通过设置访问密码或使用加密技术，可以限制对电子信息档案的访问，并防止未授权的人员进行篡改、修改或删除等操作。在加密方面，可以采用对称加密或非对

称加密等技术，对敏感信息进行加密处理，保护隐私和机密信息不被泄露。除此之外，还可以采用访问控制、审计等安全措施来进一步增强电子信息档案的安全性。例如，设置访问权限，只允许授权人员进行访问、修改、删除等操作；记录访问日志，对所有的操作进行记录并定期审计，可及时发现异常操作并采取应对措施。

三、医院电子信息档案管理的风险

（一）技术风险

医院电子信息档案管理所依赖的技术属于高科技范畴，包括计算机硬件、软件、网络等。但这些技术发展迅速，档案管理可能出现技术更新滞后，系统故障等情况，导致信息的丢失、损坏或泄露。另外，医院电子信息档案管理还可能受到黑客攻击、病毒感染等技术风险的影响。黑客可能会试图入侵医院电子信息档案系统，窃取或篡改敏感信息，病毒也可能通过网络进入系统，对系统造成损害。此外，由于医院电子信息档案系统所依赖的技术比较复杂，维护和管理的难度也较大，如果医院缺乏专业的技术人员，就会面临技术风险的挑战[3]。

（二）操作风险

操作错误也是可能导致电子信息档案损坏或丢失的原因，如果操作人员没有得到充分的培训和指导，就有可能不慎误操作，比如误删或误修改档案信息。因此，为了避免电子信息档案的易损坏问题，医院管理人员需要采取相应的安全措施，包括加强设备和软件的安全防护、备份数据、建立恢复机制、加强操作人员的培训和考核等。这些措施可以有效地保障电子信息档案的安全性和完整性，确保其可靠性和可持续性。

（三）安全风险

随着医院信息化建设的不断发展，电子信息档案已经成为医院信息化建设的重要组成部分，而其安全风险也越来越受到关注。安全风险包括网络攻击、黑客攻击、病毒感染、操作失误、系统故障等多种因素。医院电子信息档案包含大量的患者病历、医生诊断、治疗方案等医疗信息，一旦泄露和篡改将直接威胁到医疗机构和患者的安全和利益。同时，数据的正确性和完整性也是电子信息档案管理的重要问题，数据错误和丢失将直接影响医院的正常运营。因此，保证医院电子信息档案的安全性和完整性是医院信息化建设中必须重视的问题[4]。

（四）知识产权风险

医院电子信息档案中包含了丰富的医疗知识产权，例如病例、诊断、治疗方案等，这些都是医院的核心技术和专业秘密。如果电子信息档案泄露，就会对医院知识产权产生威胁，进而影响医院的核心竞争力。

四、医院电子信息档案管理的风险控制

（一）电子信息档案的备份与恢复

备份和恢复是电子信息档案管理中非常重要的环节。在备份数据时，可以采用备份服务器的方式，即将数据备份到另外一台服务器上，保证数据的安全性。此外，为了防止备份数据也被病毒或黑客攻击，建议将备份数据存储在离线设备上，如磁带、光盘等。这样可以保证数据的可靠性和安全性，避免数据被篡改、破坏或遗失。

在建立备份机制的同时，医院还需要建立恢复机制，确保数据在灾难事件发生时可以及时恢复。为此，需要定期测试备份和恢复的过程，以确保备份的数据能够及时、完整地被恢复。医院还可以根据实际情况，制定相应的应急预案，对不同的紧急情况进行分类，明确应对方案，确保在应急情况下能够快速、有效地恢复数据，保障数据的安全性和完整性，以确保医院业务的连续性。

（二）管理制度建设

建立规范的操作流程：建立电子档案的建档、管理、查询、维护、备份等规范化操作流程，确保操作流程的科学性和规范性。这需要结合实际情况，根据系统特点和医院实际需求，制定具体的操作流程和操作指南，并进行持续的优化和改进。

1.制定权限管理制度。制定责任人及操作人员的权限管理制度，规定各个角色的权限和职责，明确各个岗位的职责范围，避免人员越权访问和操作，确保数据的安全性和可靠性。同时，要实行审计制度，对操作记录进行监控和审计，保障数据的安全性和合法性。

2.规范操作流程。规范操作流程，明确各个岗位职责，建立岗位责任制，加强对相关人员的培训和考核，提高人员的素质和业务水平。同时，要注重对医务人员的安全教育和宣传，提高安全意识，防止信息泄露和丢失等安全事件的发生。

3.定期维护与备份。定期进行维护和备份，确保系统的稳定性和数据的完整性。备份数据需要存储在安全的地方，采取可靠的备份方式，确保备份数据的可靠性和完整性。同时，还需要建立灾难恢复机制，为系统遭遇灾害或其他不可预见的情况提供可靠的保障。

（三）认证控制

认证控制是指通过身份验证和访问控制等措施，来确保系统只允许经过授权的用户进行访问和操作，从而保障

系统的安全性和数据的保密性。在电子信息档案系统中，采用较为严格的认证控制机制非常重要，因为这些系统存储了大量的敏感信息，例如患者的病历、药品处方等。如果这些信息泄露或被未经授权的人员访问，将会对患者造成不可预知的风险和严重后果。

身份验证是认证控制的第一步，其目的是确认用户的身份和访问权限。对于电子信息档案系统，可以使用多种身份验证技术，例如口令、生物识别技术（如指纹和虹膜识别）和智能卡等。其中，智能卡是一种非常安全和方便的身份验证方式，它将用户的身份信息存储在卡片中，可以在插入读卡器时进行验证。通过使用这些技术，可以确保只有授权用户才能访问和操作电子信息档案系统。

访问控制是认证控制的第二步，其目的是限制用户访问敏感信息的范围和方式。在电子信息档案系统中，访问控制可以通过实现细粒度的权限控制来实现。这意味着可以针对每个用户和每个数据对象分别设置不同的权限，以确保只有授权用户才能访问和操作相应的数据。此外，还可以通过记录用户的访问历史来监测和检测不正常的访问行为，以及设置实时告警机制，以便及时发现和应对安全漏洞和威胁，帮助保护患者的隐私和医疗数据的安全性，为患者提供更加安全和可靠的医疗服务。

（四）技术安全控制

除了认证控制外，电子信息档案系统还存在着一些技术安全问题，如系统备份与恢复、数据存储加密和网络安全等。针对这些问题，需要采取相应的措施来保障系统的安全性和数据的完整性、保密性和可用性。

第一，系统备份与恢复是保障系统可用性和数据完整性的重要方法。为了确保系统在遭受灾害或其他意外事件后能够迅速恢复正常工作，需要建立健全的备份与恢复机制。具体措施包括定期备份数据，选择合适的备份介质和方式，并测试恢复能力以确保备份数据的可用性和准确性。

第二，对于电子信息档案系统中的数据存储，为了确保数据的安全性和隐私性，需要采用可靠的技术方法进行加密存储。一般情况下，可以使用对称加密和非对称加密相结合的方式，对数据进行加密处理，并设置访问控制，仅允许授权人员访问和处理数据。

第三，要对网络安全进行管理，包括加强网络设备和软件的安全防护，实行访问控制、规范管理行为等。具体措施包括采用网络安全设备和软件，如防火墙、入侵检测系统、反病毒软件等，对网络进行安全防护；实施访问控制，限制用户访问权限，并对访问行为进行监控和记录；加强网络安全培训，提高员工的安全意识，避免人为因素导致的安全事件的发生，有效地保障电子信息档案系统的安全性和可用性，确保医院的信息安全和医疗质量。

（五）安全意识培养

医院电子信息档案管理的安全意识培养是一个非常重要的任务，因为现代医疗系统涉及大量的敏感信息，如病历、医疗报告、药物处方等。这些信息需要得到保护，以防止非授权访问、修改、泄露和丢失。因此，为了确保医疗数据的安全，必须加强医院职工的安全管理意识，提高安全意识水平，以便避免发生任何安全事件。

为了实现这一目标，可以采取一系列措施，例如定期开展安全培训。这种安全培训可以针对医院各个部门的不同职位进行，以确保每个员工都能够了解有关信息安全的最新知识和最佳实践。通过这种培训，员工可以学习到如何保护医疗数据、如何使用密码和加密技术、如何处理安全漏洞等相关内容。此外，可以加强安全宣传，以提高员工之间的信息共享和安全意识。安全宣传可以采用多种形式，如海报、通知、邮件和内部网站等，以传达关于信息安全的重要性和医院安全政策的相关信息。

医院可以制定相应的权限管理制度，规定各个岗位的职责和权限，明确操作人员的操作范围和操作权限。在操作过程中，医院还应该严格按照操作规程进行操作，确保每一步操作都符合规范和流程要求。此外，医院还可以采用技术方法，如日志记录、审计等，对操作过程进行记录和监管。建立相应的纠错机制，及时发现和纠正操作中的错误，使得操作人员随时提高安全意识，保障电子信息档案的安全性和完整性。

五、结语

综上所述，电子信息档案管理是医院信息化建设的重要组成部分。面对电子信息档案管理的风险与挑战，有效防范、解决存在的问题势在必行。

参考文献

[1]许舟洋.大数据时代电子信息档案管理存在问题与改进建议[J].办公自动化,2023,28(01):40-43,61.

[2]黄敏静.电子信息档案管理在医院业务中的应用及控制[J].行政事业资产与财务,2022(24):100-102.

[3]许志颖.加强医院电子信息档案建设和管理的思考[J].黑龙江档案,2022(01):186-188.

[4]郝蕊,郑洁,李娜.基于互联网+平台的医院档案电子信息管理系统设计与应用[J].中国医学装备,2021,18(02):90-93.