

医院信息化进程中数据安全与隐私保护研究

王瑞明

天津市人民医院 天津 330026

摘要: 随着信息技术的飞速发展,医院信息化进程不断加速,医疗数据的收集、存储、处理、传输和共享变得日益频繁。然而,这一进程也伴随着数据安全与隐私保护的严峻挑战。医疗数据包含患者的个人信息、病史、诊断结果等敏感内容,一旦泄露或滥用,将对患者造成严重的伤害,并影响医疗服务的连续性和质量。因此,研究医院信息化进程中的数据安全与隐私保护问题具有重要意义。

关键词: 医院信息化;数据安全;隐私保护

引言

医院信息化是提高医疗服务效率、优化资源配置、提升医疗质量的重要手段。然而,随着医疗数据的海量增长和广泛应用,数据安全与隐私保护问题日益凸显。保护患者隐私是医疗伦理和法律的基本要求,也是医院信息化建设的核心内容之一。本研究旨在探讨医院信息化进程中数据安全与隐私保护的现状、挑战及应对策略。

1 医院信息化进程中数据安全与隐私保护的现状

1.1 数据安全与隐私保护意识增强

近年来,随着相关法律法规的不断完善和社会公众对隐私保护意识的显著提高,医院对数据安全与隐私保护的重视程度也在持续提升。这一变化不仅体现在医院管理层的决策中,也深入到了医院的日常运营和文化建设中。许多医院开始积极制定和完善信息安全管理制,这些制度不仅明确了各部门和人员在数据安全与隐私保护方面的职责,还规定了具体的操作流程和应急响应机制。通过制度的建立和完善,医院确保了在数据安全与隐私保护方面有章可循、有据可查。同时,医院也加强了对员工的培训和教育。通过定期举办信息安全知识讲座、开展信息安全演练等活动,医院提高了全员的安全意识,使员工能够充分认识到数据安全与隐私保护的重要性,并在实际工作中自觉遵守相关规定和操作流程^[1]。此外,医院还积极与社会各界合作,共同推动数据安全与隐私保护工作的深入开展。例如,与科研机构合作开展相关研究,与监管部门保持密切沟通,及时了解最新的法律法规和政策要求,确保医院的数据安全与隐私保护工作始终走在前列。

1.2 技术手段不断进步

在技术手段方面,医院也在不断探索和创新,以更好地保护医疗数据的安全。加密技术、访问控制技术、防火墙、入侵检测系统等传统安全措施已经得到了广

泛应用,并且不断得到优化和升级。这些技术手段的有效应用,为医院的数据安全与隐私保护提供了有力的技术支撑。同时,随着区块链、零知识证明、同态加密等先进技术的发展,医院在数据安全与隐私保护方面有了更多的选择。区块链技术以其去中心化、不可篡改的特点,为医疗数据的存储和传输提供了更高的安全性;零知识证明技术可以在不泄露数据内容的情况下证明数据的某些属性,有效保护了患者的隐私;同态加密技术则允许在加密的数据上进行计算,而无需解密,为医疗数据的处理和分析提供了新的思路。医院正在积极关注这些先进技术的发展动态,并尝试将其应用到实际的数据安全与隐私保护工作中。通过不断引入新技术、新手段,医院将不断提升数据安全与隐私保护的水平,为患者的医疗信息安全提供更有力的保障。

2 医院信息化进程中数据安全与隐私保护的挑战

2.1 数据泄露风险增加

随着医疗数据的电子化、网络化和共享化,数据泄露的风险也在持续攀升。医疗数据作为医院运营的核心资产,包含了患者的个人信息、病史记录、诊断结果等高度敏感的内容。一旦这些数据被非法获取或滥用,将给患者带来严重的隐私侵犯和经济损失,甚至可能危及患者的生命安全。数据泄露的风险来源多种多样。黑客攻击是其中最为常见且威胁最大的一种。黑客可能利用系统漏洞、弱密码、恶意软件等手段,非法侵入医院的信息系统,窃取或篡改医疗数据。此外,内部人员泄露也是不容忽视的风险。一些员工可能因疏忽大意、利益驱使或恶意行为,将医疗数据泄露给外部人员或机构。同时,系统漏洞也是导致数据泄露的重要原因。随着信息技术的不断发展,新的漏洞和攻击手段层出不穷,给医院的信息安全带来了严峻的挑战。数据泄露的后果十分严重。除了给患者带来隐私侵犯和经济损失外,还可

能引发社会恐慌和信任危机。一旦医疗数据被泄露,患者可能对医院失去信任,选择其他医疗机构就诊,从而影响医院的声誉和业务发展。因此,医院必须高度重视数据泄露风险,采取有效措施加强数据安全防护。

2.2 数据访问控制难度大

在医院信息化进程中,医疗数据的访问权限管理变得日益复杂。随着医院信息系统的不断完善和功能的不断拓展,医疗数据的种类和数量也在不断增加。不同部门、不同岗位的人员对数据的访问需求各不相同,如何确保只有授权人员能够访问特定数据成为了一大挑战。一方面,医院需要确保医疗数据的可用性和便捷性,以便医护人员能够及时、准确地获取所需信息,为患者提供优质的医疗服务^[2]。另一方面,医院又必须严格控制数据的访问权限,防止未经授权的人员获取或滥用医疗数据。这需要医院在数据访问控制方面做出精细化的管理,确保数据的访问既方便又安全。然而,实现这一目标并不容易。医院需要建立完善的访问控制机制,明确各部门和人员的访问权限,并加强对访问行为的监控和审计。同时,医院还需要定期对访问控制策略进行评估和调整,以适应医院业务发展和信息安全需求的变化。此外,医院还需要加强对员工的培训和教育,提高员工的安全意识和责任意识,确保员工能够自觉遵守访问控制规定,共同维护医疗数据的安全。

2.3 法律法规遵循难度大

随着医疗数据保护法律法规的不断完善,医院在遵循法律法规方面面临着前所未有的挑战。医疗数据作为个人隐私的重要组成部分,其保护不仅关系到患者的权益,也关乎医院的法律责任和社会信誉。因此,如何确保医疗数据的收集、存储、处理、传输和共享都符合法律法规的要求,已成为医院信息化建设中的一项重要课题。首先,医疗数据保护法律法规的频繁更新和变化,使得医院需要不断关注和适应新的法律要求。这不仅要求医院具备敏锐的法律意识,还需要投入大量的人力和物力去研究和解读新的法律法规,以确保医院的信息化建设与法律法规保持同步。其次,医疗数据的收集、存储、处理、传输和共享涉及多个环节,每个环节都可能存在法律风险。例如,在数据收集过程中,医院需要确保患者知情同意,并明确告知数据的使用目的和范围;在数据存储和处理过程中,医院需要采取有效的技术措施和管理措施,防止数据被非法获取或滥用;在数据传输和共享过程中,医院需要与数据接收方签订保密协议,并明确数据的使用权限和责任^[3]。这些环节的法律要求复杂且细致,医院需要建立完善的法律合规体

系,确保每个环节都符合法律法规的要求。再者,医院还需要面对不同地域、不同国家法律法规的差异和冲突。随着医疗国际化的趋势日益明显,医院可能需要与国外的医疗机构或研究机构进行数据共享和合作。然而,不同地域、不同国家的医疗数据保护法律法规可能存在差异和冲突,这给医院的法律合规工作带来了更大的挑战。医院需要仔细研究相关法律法规,制定符合各方要求的法律合规方案,以确保数据共享和合作的顺利进行。

3 医院信息化进程中数据安全与隐私保护的应对策略

3.1 加强制度建设与人员培训

医院在信息化进程中,数据安全与隐私保护是不可或缺的一环。为了有效应对这一挑战,医院应首先建立完善的信息安全管理制度。这些制度应明确各部门和人员在数据安全与隐私保护方面的具体职责,确保每个环节都有章可循、有据可查。同时,制度还应涵盖数据分类、存储、处理、传输和销毁等全生命周期的管理要求,确保医疗数据在整个生命周期内都得到妥善保护。除了制度建设,人员培训也是至关重要的。医院应定期对员工进行信息安全意识培训,提高全员对数据安全与隐私保护的认知和重视程度。培训内容可以包括信息安全法律法规、医院信息安全管理规定、常见的信息安全威胁和防范措施等。通过培训,使员工能够自觉遵守相关规定,增强信息安全意识,共同维护医院的信息安全。此外,医院还应定期开展信息安全演练和应急响应培训。通过模拟真实的信息安全事件,检验医院应对信息安全事件的能力和应急响应流程的有效性。同时,针对演练中暴露出的问题和不足,及时进行调整和优化,提高医院应对信息安全事件的实战能力。

3.2 采用先进技术手段保护数据安全

在技术手段方面,医院应积极采用加密技术、访问控制技术、防火墙、入侵检测系统等先进技术手段来保护医疗数据的安全。加密技术可以对医疗数据进行加密存储和传输,确保数据在传输过程中不被窃取或篡改。访问控制技术可以限制对医疗数据的访问权限,确保只有授权人员才能访问特定数据。防火墙可以阻挡外部网络对医院内部网络的非法访问和攻击。入侵检测系统可以实时监测医院网络中的异常行为,及时发现并防范潜在的信息安全威胁。除了传统的安全技术手段,医院还可以探索区块链、零知识证明、同态加密等新技术在医疗数据安全与隐私保护中的应用。区块链技术具有去中心化、不可篡改的特点,可以为医疗数据的存储和传输提供更高的安全性。零知识证明技术可以在不泄露数据

内容的情况下证明数据的某些属性,有效保护患者的隐私^[4]。同态加密技术则允许在加密的数据上进行计算,而无需解密,为医疗数据的处理和分析提供了新的思路。医院应密切关注这些新技术的发展动态,积极引入和应用新技术,不断提高数据安全与隐私保护的水平。同时,医院还应加强对新技术的研究和探索,结合医院自身的实际情况和需求,定制化的开发和应用新技术,为医院的信息化建设提供有力的技术支撑。

3.3 强化数据访问控制与管理

在医院信息化进程中,数据访问控制与管理是确保医疗数据安全性与隐私的关键环节。为了有效防止未经授权的人员访问敏感数据,医院应实施严格的访问控制策略。这一策略应明确规定不同级别、不同岗位的人员对医疗数据的访问权限,确保只有经过授权的人员才能访问特定数据。为了实现这一目标,医院可以采用基于角色的访问控制(RBAC)和基于属性的访问控制(ABAC)等模型来管理用户对数据的访问权限。RBAC模型通过为用户分配不同的角色,并根据角色赋予相应的访问权限,从而简化了权限管理过程,提高了管理效率。而ABAC模型则根据用户的属性(如职位、部门、职责等)以及数据的属性(如敏感级别、分类等)来动态决定用户的访问权限,提供了更细粒度的访问控制。除了实施严格的访问控制策略,医院还应建立审计追踪机制。这一机制应能够记录数据的访问和使用情况,包括访问时间、访问人员、访问目的以及访问结果等信息。通过审计追踪,医院可以事后追溯和审查数据的访问行为,及时发现并处理潜在的违规访问或数据泄露事件。

3.4 遵循法律法规要求

随着医疗数据保护法律法规的不断完善,医院在信息化进程中必须密切关注法律法规的动态变化。医院应设立专门的法律合规部门或岗位,负责跟踪和研究相关法律法规的最新动态,及时调整和完善医院的信息安全管理制度和流程,确保医院的信息化建设与法律法规要

求保持一致。同时,医院还应加强与监管机构的沟通合作。监管机构是医疗数据保护法律法规的制定者和执行者,医院应主动与监管机构建立联系,接受其指导和监督。通过定期向监管机构报告医院的信息安全状况、参与监管机构组织的培训和研讨会等方式,医院可以及时了解监管机构的最新要求和政策导向,共同维护患者隐私安全^[5]。此外,医院还应加强对员工的法律法规培训。员工是医院信息化建设的参与者和执行者,他们的法律法规意识直接关系到医院的信息安全水平。医院应定期组织法律法规培训活动,提高员工的法律法规意识和合规意识,确保员工在工作中自觉遵守相关法律法规要求,共同维护医院的信息安全和患者隐私安全。

结束语

医院信息化进程中的数据安全与隐私保护问题是一个复杂而重要的课题。通过加强制度建设与人员培训、采用先进技术手段保护数据安全、强化数据访问控制与管理以及遵循法律法规要求等措施,可以有效提升医院数据安全与隐私保护水平。未来,随着信息技术的不断发展和医疗数据保护法律法规的不断完善,医院数据安全与隐私保护工作将面临更多的挑战和机遇。

参考文献

- [1]付航,王成增,王素凡,蒋帅,段彦然.大型公立医院参与主动健康的路径探讨[J].中国医院管理,2023,43(06):84-86.
- [2]邢会强.元宇宙的“网信安全”与法律适用[J/OL].法律科学(西北政法大学学报),2023(04):1-13[2023-06-08].
- [3]尤丽珏.医院移动医疗服务中患者隐私保护研究[J].中国医疗器械信息,2018,12(5):110-111.
- [4]王伟.移动医疗时代患者的隐私安全[J].青年记者,2016,12(32):17-18.
- [5]甘贝贝.监测报告显示:移动医疗或成改善服务重要抓手[J].吉林医学信息,2016,11(15):160-170.