基于大数据的医疗信息隐私保护探究

孙乐乐
宁夏医科大学总医院　宁夏　银川　750000

摘　要：大数据在医疗领域应用广泛，提升了医疗服务效率和质量。然而，医疗信息隐私面临数据存储、共享及数据分析过程中的泄露风险。为保护隐私，可采用数据加密技术、差分隐私技术和安全多方计算技术等手段。同时，医疗机构需强化人员管理与培训，规范数据处理流程，确保隐私保护贯穿数据全生命周期。此外，建立隐私保护评估机制，定期评估和优化隐私保护措施，对于持续提升医疗信息隐私保护水平至关重要。

关键词：大数据；医疗信息；隐私保护；探究

引言：随着大数据技术在医疗领域的深入融合，医疗信息的处理和分析迎来了前所未有的机遇与挑战。大数据不仅极大地提升了医疗服务的效率和质量，还促进了医疗研究的深入发展。然而，医疗信息的隐私保护问题也随之凸显，成为制约大数据在医疗领域广泛应用的关键因素。医疗信息具有高度的敏感性和私密性，一旦泄露，可能对患者造成不可估量的损失。因此，探索有效的医疗信息隐私保护技术，规范数据处理流程，强化人员管理与培训，建立隐私保护评估机制，对于保障患者隐私权益、推动医疗大数据的健康发展具有重要意义。

1 大数据在医疗领域的应用及特点

随着信息技术的迅猛发展，大数据已逐渐成为推动各行各业变革的重要力量，医疗领域也不例外。大数据在医疗领域的应用广泛而深入，不仅改变了传统的医疗服务模式，还极大地提升了医疗服务的效率和质量。（1）大数据在医疗领域的应用是多方面的，其中电子病历系统是其最为基础且重要的应用之一。电子病历系统通过整合患者的基本信息、诊断结果、治疗过程、药物过敏史等多维度数据，为医生提供了一个全面、准确、实时的患者信息库。这不仅方便了医生快速了解患者的病史和现状，还为医生制定个性化的治疗方案提供了有力支持。电子病历系统的普及和应用，极大地提高了医疗服务的连续性和协同性，使得患者在不同医疗机构之间的就诊体验更加顺畅。（2）除了电子病历系统，大数据还在临床决策支持系统中发挥着重要作用。临床决策支持系统通过分析大量病例数据，挖掘出疾病的发生、发展和转归规律，为医生提供科学、准确的诊疗建议。这种基于数据的决策支持，有助于医生在面对复杂病例时做出更加合理、有效的治疗决策，提高医疗服务的专业性和安全性。（3）在疾病预测与预防方面，大数据也展现出了其独特的优势。通过对海量医疗数据的深度挖掘和分析，大数据可以揭示疾病的流行趋势、高危人群和潜在风险因素，为政府和医疗机构提供科学的防控策略。这种基于数据的预测和预防，有助于提前采取干预措施，降低疾病的发生率和死亡率，提高公众的健康水平。（4）大数据在药物研发过程中也发挥着举足轻重的作用。传统的药物研发过程耗时长、成本高、成功率低，而大数据的应用可以大大加速这一进程。通过筛选潜在药物靶点、评估药物疗效和安全性等，大数据为药物研发提供了更加精准、高效的方法和手段，有助于缩短药物研发周期，降低研发成本，提高药物的成功率和市场竞争力。（5）医疗大数据不仅应用广泛，还具有一些独特的特点。首先，数据量大是医疗大数据的显著特点之一。随着医疗信息化的不断推进，医疗机构产生的数据量呈现出爆炸式增长的趋势。这些海量数据包含了丰富的医疗信息和知识，为医疗研究和决策提供了宝贵的资源。其次，医疗大数据具有多样性。医疗数据不仅来源于电子病历、临床决策支持系统等结构化数据，还来源于医学影像、生理信号等非结构化数据。这种多样性使得医疗数据的整合和分析更加复杂，但也为医疗研究和决策提供了更加全面、多维的信息支持。再者，医疗大数据具有高价值性。医疗数据蕴含着丰富的医疗知识和经验，对于医疗研究、疾病预测、药物研发等方面都具有重要的意义。然而，这种高价值性也使得医疗数据成为不法分子觊觎的目标，加强医疗数据的隐私保护显得尤为重要。最后，医疗大数据具有时效性强等特点。医疗数据的产生和更新速度非常快，这就要求医疗机构和数据处理机构能够及时、准确地获取和处理这些数据，以支持医疗决策和服务的实时性需求[1]。

2 医疗信息隐私面临的威胁

2.1 数据存储环节的风险

医疗信息通常被存储在医疗机构的数据中心或云端服务器中，以便于医生、护士等医疗人员随时访问和使用。然而，数据存储设备本身可能存在物理安全漏洞，这是医疗信息隐私泄露的一大风险源。服务器可能因被盗、损坏或自然灾害等原因导致数据丢失或泄露。一旦服务器受到物理攻击或损坏，存储在其上的医疗信息就可能落入不法之手，被用于非法目的。除了物理安全漏洞，存储系统的软件也可能存在漏洞。黑客可以利用这些漏洞入侵系统，获取医疗信息。随着黑客技术的不断进步，他们越来越擅长利用软件漏洞进行攻击，这使得医疗信息系统的安全性面临严峻挑战。此外，数据备份和恢复过程中也可能出现隐私泄露问题。如果备份数据未妥善保管，被未经授权的人员获取，那么患者的隐私就可能被泄露。

2.2 数据共享带来的隐私隐患

在医疗研究、远程医疗等场景中，医疗信息需要在不同机构和人员之间进行共享。然而，数据共享过程中存在着隐私泄露的风险。一方面，数据的控制权难以有效保障。在共享过程中，数据可能会被共享给不具备相应权限的人员，导致患者隐私被泄露。另一方面，不同机构的数据安全标准和管理水平参差不齐。一旦接收方的数据安全措施不到位，就容易导致数据泄露。例如，在多中心的医疗研究项目中，各参与机构的数据整合和共享过程中，若缺乏严格的隐私保护机制，患者信息就可能被泄露给未经授权的研究人员或第三方机构。

2.3 数据分析过程中的隐私泄露

大数据分析技术在医疗领域的应用越来越广泛，它能够帮助医疗人员挖掘医疗数据的潜在价值，提高医疗服务的效率和质量。然而，大数据分析技术也带来了隐私泄露的风险。分析人员可能会在不经意间泄露患者隐私，如在研究报告中使用了可识别患者身份的信息。这种泄露可能是无意的，但后果却是严重的，因为它可能导致患者的个人隐私被公开曝光。此外，一些先进的数据分析算法，如关联分析、聚类分析等，可能会从看似无关的数据中推断出患者的敏感信息。这些算法能够挖掘出数据之间的隐含关系，从而揭示出患者的个人隐私。例如，通过分析患者的购药记录、就诊记录等信息，可能会推断出患者的疾病状况、生活习惯等敏感信息。这种推断性的隐私泄露更加隐蔽和难以防范，因此需要对数据分析过程进行严格的监管和控制[2]。

3 基于大数据的医疗信息隐私保护技术

3.1 数据加密技术

数据加密是保护医疗信息隐私的基础手段。在医疗信息系统中，通过对医疗数据进行加密处理，将明文数据转换为密文，确保只有拥有正确密钥的人员才能解密获取原始数据。这一技术有效防止了未经授权的人员访问和泄露医疗信息。（1）常见的加密算法包括对称加密算法和非对称加密算法。对称加密算法，如高级加密标准（AES），以其加密和解密速度快、效率高而著称，但密钥管理相对复杂，需要确保密钥的安全传输和存储。非对称加密算法，如Rivest-Shamir-Adleman（RSA）算法，则具有密钥管理相对简单的优势，但加密和解密速度较慢。（2）在实际应用中，医疗机构可以根据数据的特点和使用场景选择合适的加密算法。对于需要高效处理的大量医疗数据，对称加密算法可能是更好的选择；而对于需要确保密钥安全性的场景，非对称加密算法则更为适用。此外，还可以结合使用多种加密算法，形成多层次、多级别的加密保护，进一步提高数据的安全性。

3.2 差分隐私技术

差分隐私是一种新兴的隐私保护技术，它通过向数据中添加噪声来保护个体数据的隐私。在医疗数据分析过程中，差分隐私技术能够确保即使攻击者掌握了除某一条记录之外的所有数据，也无法准确推断出该记录是否存在于数据集中。差分隐私技术的核心思想是在数据分析过程中引入随机性，使得个体数据对分析结果的影响变得微小且难以察觉。这一技术能够在保证数据分析结果准确性的前提下，有效保护个体数据的隐私。在医疗数据的统计分析和数据挖掘场景中，差分隐私技术具有广泛的应用前景。

3.3 安全多方计算技术

安全多方计算技术是一种允许多个参与方在不泄露各自隐私数据的前提下，共同进行计算的技术。在医疗领域，这一技术具有重要的应用价值。多个医疗机构或研究机构可以利用安全多方计算技术，在不共享原始数据的情况下，进行联合数据分析和模型训练。例如，不同医院可以共同分析患者的疾病数据，以发现疾病的流行规律和治疗方法。通过安全多方计算技术，各医院可以在不泄露各自患者数据的情况下，共同计算出疾病的发生率、治愈率等关键指标，为医疗研究和决策提供有力支持。这一技术不仅保护了患者的隐私权益，还促进了医疗数据的共享和利用，提高了医疗服务的效率和质量[3]。

4 医疗信息隐私保护的策略

4.1 强化人员管理与培训

医疗机构的工作人员是接触和处理医疗信息的直接参与者，他们的安全意识和操作规范对医疗信息的隐私

安全具有至关重要的影响。因此，加强对工作人员的管理和培训，提高他们的隐私保护意识和数据安全技能，是医疗信息隐私保护的首要任务。（1）培训内容应全面而深入，既要包括医疗信息隐私保护的重要性，使工作人员充分认识到隐私泄露可能带来的严重后果，也要涵盖相关法律法规、行业规范和道德准则，确保工作人员在处理医疗信息时能够遵纪守法、恪守职业道德。同时，还应加强数据安全操作流程的培训，使工作人员能够熟练掌握数据安全的操作技能，防止因操作不当导致隐私泄露。（2）建立严格的人员权限管理制度也是强化人员管理的重要环节。医疗机构应根据不同岗位的工作职责和需要，明确不同岗位人员的权限，确保只有经过授权的人员才能访问和处理医疗信息。同时，还应加强对人员权限的监督和管理，防止内部人员违规操作导致隐私泄露。

4.2 规范数据处理流程

医疗信息的处理流程包括数据的收集、存储、处理和共享等多个环节，每一个环节都可能存在隐私泄露的风险。因此，规范数据处理流程，确保隐私保护贯穿始终，是医疗信息隐私保护的关键。（1）在数据收集阶段，医疗机构应明确收集目的和范围，仅收集必要的医疗信息，并征得患者的明确同意。同时，还应加强对数据收集过程的监督和管理，防止过度收集或非法收集医疗信息。（2）在数据存储阶段，医疗机构应选择安全可靠的存储设备和存储方式，并定期进行数据备份和安全检查，确保医疗信息的安全可靠。（3）在数据处理阶段，医疗机构应对数据进行严格的访问控制，确保只有授权人员才能进行处理。同时，还应加强对数据处理过程的监控和审计，防止数据处理过程中的隐私泄露。（4）在数据共享阶段，医疗机构应对共享数据进行严格的审核和加密处理，确保数据在共享过程中的安全。同时，还应与共享方签订隐私保护协议，明确双方的责任和义务，共同维护医疗信息的隐私安全。

4.3 建立隐私保护评估机制

医疗信息隐私保护是一个持续不断的过程，需要定期进行评估和优化。因此，建立隐私保护评估机制，定期对医疗信息隐私保护措施的有效性进行评估，及时发现和解决存在的问题，是医疗信息隐私保护的重要保障。（1）评估内容应全面而细致，包括数据加密效果、访问控制措施的执行情况、隐私保护技术的应用效果等多个方面。评估方法应科学而合理，可以采用定量分析和定性分析相结合的方式，确保评估结果的准确性和可靠性。（2）根据评估结果，医疗机构应对隐私保护措施进行调整和优化，不断提高医疗信息隐私保护的水平。同时，还应加强对隐私保护工作的宣传和教育，提高全体工作人员的隐私保护意识和责任感，共同维护医疗信息的隐私安全[4]。

结束语

随着大数据技术在医疗领域的深入应用，医疗信息的隐私保护问题日益凸显其重要性。通过数据加密、差分隐私、安全多方计算等先进技术，我们可以有效保障医疗数据的隐私安全，为医疗研究和决策提供有力支持。同时，医疗机构也应加强人员管理与培训，规范数据处理流程，确保隐私保护贯穿数据生命周期的每一个环节。此外，建立隐私保护评估机制，定期对隐私保护措施的有效性进行评估和优化，也是不可或缺的一环。未来，我们将继续探索更加高效、安全的医疗信息隐私保护技术，为医疗领域的数字化转型提供坚实保障，共同推动医疗服务的持续改进和创新发展，让医疗数据在保障患者隐私的前提下，更好地服务于人类健康事业。

参考文献

[1]张娟萍,张海亮. 大数据与数据隐私保护相关问题研究[J]. 软件,2023,44(2):81-84.

[2]冯凡. 大数据分析技术下的隐私保护[J]. 数字通信世界,2023(3):142-145.

[3]张磊,许豪勤,徐宁.刍议医疗大数据环境下的健康信息分析方法[J].信息系统工程.2019,(9):65-78

[4]肖瑗,卢雅雯,吕智慧,等.生物医疗大数据隐私安全保障机制研究[J].计算机应用与软件.2021,(2):12-18