数据主体控制个人健康信息的困境与解决对策

◆陈　明

（中国人民大学法学院，北京 100872）

【摘要】随着医疗行业的信息化、病历的电子化的不断发展，个人健康信息从庞大的信息种类中逐渐被提取，成为大家重点关注的对象。为响应国务院在《国务院办公厅关于促进“互联网＋医疗健康”发展的意见》的号召，鼓励进一步推进个人健康信息资源共享、建立健全个人健康信息安全保障体系的指导性政策文件精神，个人健康信息的安全和隐私的数据建设与存储问题越来越受关注。因个人健康信息具有高敏感性，承载了大量的个人隐私，健康医疗大数据建设又有赖于个人健康信息的汇总，故如何安全有效地保护个人健康信息和隐私，以及如何在合法合规的前提下查阅健康数据的问题逐渐受到大众的关注。本文将深入探讨这些困境，并提出一系列解决对策。

【关键词】健康信息；数据隐私；解决对策；技术创新；法律法规

在当今信息化、数字化时代，个人健康信息的收集和存储变得越来越便捷，然而，与之伴随而来的是个人健康信息的安全与隐私问题。个人健康医疗信息的特殊性体现在其敏感性更高、社会公益性更强、专业性更高、集合应用价值更大。而个人健康信息的泄露或滥用可能会对个体的生活造成严重影响，甚至危及生命。因此，如何破解数据主体控制个人健康信息的困境成了一个迫切需要解决的问题。本文将从技术、法律、教育和社会共识等多个角度探讨这一问题，并提出相应的解决对策，旨在为保护个人健康信息的安全与隐私提供有力的支持。

一、数据主体控制的技术挑战

（一）数据加密技术

数据加密技术在保护个人健康信息方面扮演着关键角色。然而，实施强大的数据加密并不是一项简单的任务，它面临着多重技术挑战。数据加密的安全性取决于所使用的加密算法的复杂性。为了有效保护个人健康信息，需要选择足够强大和复杂的加密算法，以使破解变得困难。然而，随着计算技术的不断进步，一些早期的加密算法可能会变得脆弱，因此需要不断升级和改进加密标准。密钥管理是数据加密的关键部分。强大的加密算法需要相应的密钥来加密和解密数据。密钥的生成、存储和分发必须极其安全，以防止未经授权的访问。此外，密钥管理也需要考虑如何定期轮换密钥，以进一步增强安全性。

另一个挑战是性能开销。数据加密和解密需要额外的计算资源，这可能会导致数据访问速度的降低。在医疗紧急情况下，每一秒都很宝贵，因此需要权衡安全性和性能。技术创新可以帮助解决这个问题，例如硬件加速和优化的加密算法可以减少性能开销。最后，数据加密需要标准化和跨平台兼容性。不同系统和应用程序之间需要一致的加密标准，以确保数据在传输和存储过程中不会遭受威胁。制定和采纳广泛接受的加密标准，对于数据的安全性至关重要。

（二）分布式存储系统

分布式存储系统是处理大量个人健康信息的关键。这些系统将数据分散存储在多个地点，提高了数据的可用性和冗余性，但也面临着一些挑战。分布式存储数据需要强大的网络基础设施，数据必须能够安全、高效地在不同地点之间传输和同步。网络中断或故障可能导致数据丢失或不可访问。数据一致性是一个复杂的问题，多个副本的数据需要保持同步，以确保在任何时候都可以访问最新的信息，这需要复杂的算法和协议来维护数据一致性。最后，分布式存储系统必须应对安全威胁。攻击者可能试图入侵其中一个存储节点，访问敏感数据。因此，系统需要强大的身份验证和访问控制机制。

在应对这些技术挑战时，需要密切关注不断发展的技术和标准。数据加密技术需要不断改进以抵御新的攻击手段，而分布式存储系统需要适应不断变化的网络环境。只有通过不断创新和改进，才能更好地确保数据主体对个人健康信息的控制。

二、法律法规的完善与执行

在数据主体控制个人健康信息的过程中，法律法规起着至关重要的作用。下面将深入探讨两个方面：隐私法律的制定和强化法律执行机构的职能和能力。

（一）隐私法律的制定

为了有效保护个人健康信息，国家和地区需要制定严格的隐私法律。这些法律应该明确规定如何处理个人健康信息，确保在数字化时代，个人的敏感信息不被滥用或泄露。

一方面，这些法律应明确定义个人健康信息的范围，以

防止定义模糊不清。它们应明确规定个人健康信息的构成，如医疗记录、生物识别数据、健康监测数据等，以便明确适用法律的范围。另一方面，隐私法律应确保数据主体对其个人健康信息拥有控制权。这包括明确规定数据主体的同意权，他们应该有权决定是否同意第三方访问或使用其健康信息，以及在何种情况下可以分享这些信息。法律还应该规定数据主体可以随时撤回同意的权利。

此外，法律应规定数据处理者的责任和义务。这包括要求数据处理者采取必要的技术和组织措施，以确保个人健康信息的安全性和隐私。法律还应该明确规定数据泄露或滥用的后果，包括罚款和刑事处罚，以确保数据处理者遵守法律规定。最后，隐私法律还应规定隐私侵犯的处罚和赔偿机制。这将为受到隐私侵犯的个人提供法律救济，同时也会对违反法律规定的机构产生威慑作用，鼓励他们更加谨慎地处理个人健康信息。

（二）强化法律执行机构的职能和能力

隐私法律的制定只是第一步，其有效执行同样至关重要。为了确保法律得以贯彻执行，需要强化法律执行机构的职能和能力。需要建立专门的隐私保护机构或部门，负责监督和管理与个人健康信息有关的事务。这些机构应该拥有独立性和权威性，能够对违法行为进行调查和起诉。

法律执行机构需要与其他部门合作，包括执法机构、信息技术专家和健康机构。只有通过跨部门的协作，才能更好地应对个人健康信息的风险和威胁。法律执行机构需要投入足够的资源和培训人员，以确保他们具备足够的专业知识和技能，能够有效地执行隐私法律。在加大法律执行机构执行力度的同时，还需要建立有效的举报和投诉机制，使个人能够报告隐私侵犯行为，并获得及时的支持和保护。

三、加强教育与增强隐私意识

在确保数据主体能够有效控制其个人健康信息的过程中，加强教育与增强隐私意识发挥着至关重要的作用。本节将深入探讨两个方面：健康信息安全教育和媒体与公众宣传。

（一）健康信息安全教育

健康信息安全教育是培养数据主体对其个人健康信息负责的关键工具。这种教育应该在不同年龄段和受众群体中进行，包括学校、医疗机构和社区。学校应该将健康信息安全教育纳入课程中。学生应该了解如何保护其个人健康信息，包括密码安全、隐私设置、不点击不安全的链接和附件等。教育应该强调信息分享的重要性，以及何时和如何与专业医疗人员分享健康信息。医疗机构应该向患者提供健康信息安全的培训和指导。患者应该了解医疗记录的保护和访问，以及如何有效地与医疗团队共享信息。医疗机构还可以借此机会推广安全的电子病历访问工具。

（二）媒体与公众宣传

媒体和公众宣传是增强个人健康信息安全意识的关键渠道。媒体可以通过各种形式的传播来推广健康信息安全的理念，包括新闻报道、社交媒体、广告和纪录片等。媒体可以报道个人健康信息泄露事件，以引起公众的关注和警惕。这有助于人们意识到隐私风险的真实存在，并激发其对维护健康信息安全的兴趣。广告和社交媒体活动可以传达简明扼要的健康信息安全原则，这些信息可以提醒人们定期更改密码、避免共享敏感信息等。此外，公众宣传活动可以组织健康信息安全的主题活动，如座谈会、讲座和宣传活动，以便公众可以深入了解该主题，提出问题并分享实践经验。

在健康信息安全方面，加强教育与增强隐私意识是预防隐私泄露措施中的重要一环。通过教育，人们可以更好地理解风险和防范措施，从而更好地保护个人健康信息的安全和隐私。同时，媒体和公众宣传可以推广这些理念，确保更多人受益于健康信息安全的知识。只有在广泛的教育和宣传下，人们才能共同努力，确保数字健康信息的安全和可信度。

四、社会共识的建立

在个人健康信息的管理中，建立社会共识至关重要。这种共识涵盖了产业界的道德规范和有关部门与公共组织的引导，以确保数据主体对其个人健康信息的控制能够得到广泛的认可和支持。

（一）产业界的道德规范

产业界在数字健康信息管理中发挥着关键作用。为了建立社会共识，产业界应该积极采取一系列道德规范和最佳实践。产业界应该建立透明的数据收集和使用政策，这些政策应该清晰地说明数据的来源、用途和共享方式，以便数据主体了解他们的数据将如何被处理。产业界需要确保数据的安全性，这包括加强网络安全、数据加密和访问控制，以防止数据泄露和滥用。此外，产业界还可以主动与数据主体合作，鼓励他们参与数据管理决策。这可以通过提供数据访问和控制工具，以及向数据主体解释数据用途和风险来实现。最后，产业界需要建立有效的自我监督机制。这将有助于确保公司遵守道德规范和法律法规，同时也能增强公众对数字健康信息管理的信任。

（二）有关部门与公共组织的引导

有关部门与公共组织在塑造社会共识方面发挥着重要作用。他们可以通过政策制定、监督和引导来推动数字健康信息管理的发展。有关部门应该制定明确的法律法规，以规范个人健康信息的收集、存储和使用。这些法律可以平衡数据主体的权益、科研和医疗的需求，确保数据不会被滥用。

有关部门可以鼓励产业界采用最佳实践，并提供相应的奖励和认证。 这可以激励公司更加积极地维护数据主体的权益。 此外，有关部门和公共组织可以组织研讨会和研究项目，以研究数字健康信息管理的伦理和社会影响。 这有助于促进公众对这一问题的深入理解，并形成更广泛的共识。 最后，有关部门和公共组织还可以与产业界和社会团体合作，共同制定数据伦理框架和道德准则，以确保数字健康信息管理在道德和社会责任方面达到最高标准。

通过产业界的道德规范和有关部门与公共组织的引导，可以建立广泛的社会共识，确保数字健康信息管理在保护个人权益的同时，也能够促进医疗和科研的发展。 这将为数据主体提供更多控制个人健康信息的机会，同时也保障了社会的长期利益。

五、解决对策的综合实施

为了有效解决数据主体控制个人健康信息的挑战，需要综合实施一系列对策。 本节将深入探讨两个方面：跨领域合作和长期监测与反馈机制。

(一)跨领域合作

解决个人健康信息管理的复杂问题需要跨多个领域的合作。 这包括医疗行业、信息技术领域、法律界、有关部门和社会组织等多方面的参与。 医疗行业和信息技术领域需要密切合作，以确保个人健康信息的安全和隐私。 医疗机构应该与技术公司合作，采用最佳的数据安全措施，同时技术公司应该理解医疗行业的特殊需求。 法律界的专业知识对于建立健全的法律框架至关重要。 律师、法学家和有关部门法律顾问应该与技术专家合作，制定和完善隐私法律和法规。

(二)长期监测与反馈机制

为了确保解决对策的有效实施，需要建立长期监测与反馈机制。 这些机制将不断评估措施的有效性，并根据实际情况进行调整。 监测机制可以跟踪个人健康信息管理的相关指标，如数据泄露事件的频率、隐私投诉的数量以及数据主体的满意度等。 这些指标可以帮助评估目标的达成程度。 反馈机制允许各方提出建议和改进意见，这可以通过举办研讨会、听证会和在线反馈渠道来实现，关键是确保反馈渠道的透明和易于访问。 监测与反馈机制应该及时和持续。 随着技术和社会环境的不断变化，解决对策需要及时调整，以适应新的挑战。 监测与反馈机制应该建立在独立性和专业性的基础上。 这可以通过委托第三方机构来进行监测和评估，以确保结果的客观性和公正性。

通过跨领域的合作和长期监测与反馈机制，人们可以更好地应对数据主体控制个人健康信息的挑战。 这将为个人健康信息的安全和隐私提供更可持续的保护，同时也有助于促进医疗和科研的发展。 只有通过协作和不断的改进，人们才能在数字化时代有效管理个人健康信息。

六、结束语

数据主体控制个人健康信息的困境是一个复杂而紧迫的问题。 本论文从技术、法律、教育和社会共识等多个角度提出了解决对策。 通过加强数据加密技术和分布式存储系统的应用，制定健全的隐私法律法规，提升健康信息安全的意识，以及建立产业界和有关部门的社会共识，人们可以更好地保护个人健康信息的安全与隐私。 跨领域的合作和长期监测反馈机制的建立也将有助于解决这一重要问题。 希望这些解决对策能够为确保个人健康信息的安全与隐私提供有力支持，推动数字时代的健康信息管理走向更加安全与可持续的未来。

参考文献：

[1]钟晓雯,孙占利.数据主体控制个人健康信息的困境与解决对策[J].医学与社会,2022,35(10):133-137,144.

[2]睢苏婕.个人健康医疗信息保护视阈下的数据可携权构建[J].私法研究,2021(01):201-213.

[3]粟丹.隐私保护视角下的个人健康数据监管研究[J].杭州师范大学学报(社会科学版),2021,43(01):93-103.

[4]黄浩,赖维云.重庆市城市成人烟草调查报告[M].重庆:重庆大学出版社,2018.

[5]童奥.个人健康信息存储与传输系统设计[D].北京:北京交通大学,2011.

作者简介：

陈明(1983－),男,汉族,广东韶关人,硕士研究生,研究方向:民商法学。