聚知刊出版社
JZK publishing

健康医疗数据共享中个人信息保护的风险与对策

庞林超 孙永祥 王丽娟

西南医科大学法学院，四川泸州，646000；

摘要：大数据时代背景下，健康医疗数据共享中个人信息保护的议题日益受到关注，尽管相关研究已逐渐深化，但二者之间如何平衡仍亟待解决。本文以健康医疗数据共享的阶段发展为脉络，以个人信息保护为焦点，对各阶段中所存在的风险进行梳理。笔者认为，个人信息保护应当优化知情同意机制，分层同意模式与动态同意模式相结合，同时强化健康医疗数据的去识别化处理，重塑医疗数据的监管架构，确保数据共享中的信息安全。通过研究，本文旨在为健康医疗数据的安全共享和管理提供理论指导和策略建议，推动数字医疗领域的可持续发展。

关键词：大数据；健康医疗数据；个人信息

DOI：10.69979/3029-2808.24.6.039

随着大数据技术的发展，医疗领域的数据共享和个人隐私保护问题逐渐凸显。诊疗过程中产生的数据不仅关联每位患者的诊断、治疗和预后，还与医疗机构的决策、政策制定和公共健康推广紧密相连。移动健康、可穿戴设备和物联网的普及使得数据的获取变得更为便捷和丰富，为医疗行业提供了前所未有的机会，促使个性化医疗、预测性医疗和远程医疗等创新模式的实现。然而，数据行业的快速发展也带来了安全和隐私的挑战。保护患者的个人信息，确保数据的完整性和可靠性成为了亟待解决的问题。

1 健康医疗数据及相关概念界定

1.1 健康医疗数据

所谓健康医疗数据，理论上一般认为是为实现健康医疗和公共卫生目标而生成或挖掘的数据，其范围十分广泛，包括但不限于在诊疗过程中所产生的数据。2018 年 9 月，国家卫健委发布的《国家健康医疗大数据标准、安全和服务管理办法（试行）》，明确了健康医疗大数据是指“在人们疾病防治、健康管理等过程中产生的与健康医疗相关的数据。”《信息安全技术健康医疗数据安全指南》（以下简称《健康医疗数据安全指南》）对这一概念进一步明确，将其定义为包括个人健康医疗数据以及由个人健康医疗数据加工处理之后得到的健康医疗相关数据。在众多学术文献和政策文件中，健康医疗数据的范围和特性存在多种阐释，这种定义的深化和调整似乎成为必然。随着基因测序、生物标志物检测等新兴技术的应用，健康医疗数据的界限将进一步扩展，以反映现代医疗健康的复杂性和多维性。

1.2 个人信息

个人信息是指能够识别个体身份或反映个体活动的任何信息。信息的性质无时无刻不处于动态之中，何为信息无法脱离相应场景做抽象判断。个人信息的范围并不存在一个“预先”的精准界定。由于技术的迅速发展，原本不属于个人信息范畴的数据，通过技术手段的整合和分析，可能转变为能够识别个体的敏感信息。另一方面，个人、组织和社会对于个人信息保护的认知和期望也在不断变化。因此，个人信息的界定、保护及其法律框架的设计不仅处于动态之中，更需要多方的合作和努力，包括法律、技术和社会伦理等多个层面的综合考量和协调。

1.3 健康医疗数据中的个人信息

健康医疗数据中的个人信息不仅仅包括患者的基本信息，还涵盖了医疗诊断、治疗记录、药物使用、实验室检测结果和影像资料等诊疗过程中产生的信息。这些数据对于医疗资源的优化、服务质量的提高和医学研究的推动都具有关键作用。进一步而言，在考虑某一疾病的新药物或治疗方法的研发和评估时，健康医疗数据为研究人员提供了一个实证基础，使其能够在真实的治疗环境中评估新药物或治疗方法对某类患者的效果。

2 健康医疗数据共享中个人信息面临的风险

2.1 健康医疗数据共享采集阶段之不当收集风险

在健康医疗数据的采集阶段，个人信息处于多重风险之中。首先，在授权机制方面，理论上知情同意模式能为公民隐私保护提供理想状态下的规范构造，赋予患者对个人健康信息的控制权，以确保健康医疗数据的安全性。但在实际操作中，医疗机构在取得患者授权时往往过于注重完成格式化告知，而忽视了确保患者能够充分理解所告知的内容。患者往往在未充分理解的情况下被动地同意其个人信息和数据的收集，这无疑削弱了知

情同意的实质意义。并且，在当前“点击同意”或“浏览同意”的同意机制设计中，患者不同意即退出，并无与医疗机构协商之余地，这实际上是对患者意愿的裹挟，未能真正尊重和保障用户的选择权和决定权，反而加剧了公民与医疗机构在信息保护方面的能力势差。其次，数据采集的多种方式，包括被动采集、主动提交以及通过可穿戴医疗检测设备采集数据等，每种方式都伴随着不同程度的个人信息安全隐患。

2.2 健康医疗数据共享使用阶段之不当利用风险

在数据共享使用阶段，个人信息的风险主要显现于数据的二次处理和再次共享可能导致个人信息的收集和传输失控。特别是在缺乏有效监管和控制机制的背景下，数据的接收方可能未能重新获得个人的知情同意，或者即便获得了个人的授权与同意，也难以确保其对数据的使用范围、处理方式和处理目的的准确性。然而，《个人信息保护法》第 23 条已对他人个人信息的二次处理情况作出明确规定。个人信息处理者在向其他个人信息处理者提供其处理的个人信息时，应告知个人接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并获得个人的单独同意。若接收方变更原先的处理目的、处理方式，应依照法律规定重新获得个人的同意。从法律规定的角度来看，对已收集的个人信息的二次处理也需得到患者的授权。然而，在实际操作中，数据的二次处理和利用往往缺乏透明度，患者难以得知其个人信息是否被滥用或医疗机构是否完全依据法律规定征求了患者的同意。个人在数据被共享后，彻底丧失对其个人信息的控制，从而使得个人的信息安全面临严重的威胁。

除此之外，在健康医疗数据的共享使用中，个人信息的的脱敏或者匿名化处理之后存在着被重新识别的风险。尽管《个人信息保护法》对个人信息的定义中不包括匿名化处理后的信息，对其进行共享无需考虑《个人信息保护法》的系列规定。然而，从技术层面来讲，绝对完美、牢不可破的匿名化技术是不存在的。即使完全按照相关规定对个人信息进行匿名化处理，也无法确保完全消除个人信息的识别风险。随着技术的进步，新的识别方法和大数据分析技术可能会威胁到原本被认为是匿名的数据的隐私。伪匿名化，即数据中包含编码或加密的个人识别信息，也可能在攻击者获得解码或解密方法时导致个人信息的泄露。因此，在处理敏感信息时，除了执行匿名化处理外，还应考虑采取更为严格的数据保护措施，以确保个人信息的安全和隐私得到更为全面和有效的保护。

2.3 健康医疗数据共享存储阶段的信息泄露风险

在数字医疗领域的广泛背景下，个人医疗健康数据的泄露问题日益突出。以美国一家提供家庭医疗服务的企业 Patient Home Monitoring 为例，由于云端配置的错误，导致存储于亚马逊 S3 服务器中的 47GB 健康医疗数据意外泄露，预计影响至少 150,000 名患者。泄露的数据包括血液测试结果、患者的姓名、家庭住址、医生信息以及病例管理记录等多方面的个人和医疗信息，这种泄露无疑是对个人隐私的严重侵犯。在中国，医疗机构的信息孤岛问题也相当严重，即便是在同一家医院内部，信息共享也面临诸多困难。尽管众多移动医疗应用程序的出现为用户提供了便利，但同时也积累了大量的个人健康医疗数据。用户往往只看到了这些产品的工具属性或平台属性，却忽视了个人数据的安全问题，不清楚这些数据最终流向何处，或被用于何种目的，这无疑加大了个人健康医疗数据泄露的风险。

3 健康医疗数据共享中个人信息保护风险之应对方案

3.1 分层同意和动态同意相结合模式的适用

分层同意是指以参加者对信息需求的深入程度为标准对信息作出纵向分类。通过信息分类和场景风险的评估策略，参与者的数据被细致地分级。场景风险评估则重点考虑了不同场景下个人信息保护的侧重点。例如，在线交易场景中的风险与在物理存储中的风险可能存在显著差异。参与者的信息按照不同的层级进行管理，每个层级都有其特定的披露和同意标准，以确保参与者知情权的实际行使。

动态同意模式则主张运用现代网络信息技术手段，在 Biobank 和参加者之间搭建一个交流平台，使信息披露与知情同意成为一个持续、动态、开放的过程。借助这一技术平台，参加者可以随时了解研究的最新信息，并自由选择同意加入（Opt In）或退出（Opt Out）。在此模式中，参加者被赋予核心地位，从而加强了与研究者之间的交流，转变为研究的合作者，而非仅仅是消极被动的参与者。信息披露的水平显著提高，持续的披露确保了参加者的同意基于充分的知情，弥补了概括同意模式下信息披露的不足，满足了法律对于同意的最高标准要求。

通过分层同意与动态同意的结合，个人健康医疗数据信息持有者基于个性化选择，自主决定是否给予同意，从而避免了“知情-同意”机制的形式主义，增强了授权的有效性，实现了意愿自治。与传统知情同意模式相比，这一模式减轻了信息持有者阅读过量信息的负担，更好地保护了信息持有者的知情权。这种持续、动态的信息交流和决策机制，确保了知情同意的真实性和有效

性，避免了传统模式下由于信息不足或过时导致的同意无效的风险。

3.2 加强数据去识别化建设

健康医疗数据去识别化在当前数字化时代显得尤为重要，其构成了健康医疗数据安全与有效利用的基石。健康医疗数据去识别化通过技术手段剔除或替换数据中的个人识别信息，使得数据在保留其原有价值的同时，降低了个人隐私泄露的风险，不仅有助于保护个人隐私，避免数据泄露带来的法律风险和社会负面影响，同时也为医疗研究、公共卫生决策和医疗服务创新提供了宝贵的数据资源。而健康医疗数据去识别化的实施不仅仅是一个技术处理过程，其中涵盖技术、法律和管理多个维度。

在技术层面，实现健康医疗数据去识别化需采纳先进的算法和工具，如差分隐私、同态加密和安全多方计算等，以确保在不泄露个人识别信息的前提下对数据进行分析和处理，保障数据的原有价值和可用性。

管理层面的完善数据管理和监控机制，包括明确的数据治理政策、数据所有权和责任的确立，以及严格的数据质量和安全控制，是确保健康医疗数据安全、完整和准确的关键，建立严格的数据访问与使用权限制度，确保只有经过授权的人员能够访问和处理数据；同时，制定详细的数据安全管理规范与操作指南，明确数据去识别化、加密、传输、存储、使用等各环节的安全要求。

在法律法规层面，完善相关法律法规与标准，明确数据去识别化的技术要求与评估标准，为健康医疗数据去识别化提供明确的法律依据与技术指导。同时，加强对健康医疗数据处理与使用的监管，确保所有涉及个人信息处理的活动都符合法律法规与标准的要求。通过综合运用技术、管理与法律法规措施，为健康医疗数据的安全共享与使用提供全方位的保障，确保在实现健康医疗数据的价值利用的同时，充分保护个人信息的安全与隐私。

3.3 优化健康医疗数据监管模式

正如上文所述，健康医疗数据共享在促进医疗资源优化配置、提高医疗服务效率等方面具有重要价值，但同时，随之而来的个人信息泄露和数据安全风险仍不容忽视。为此，政府监管者的角色显得尤为关键。2018年，国家卫建委发布了《国家健康医疗大数据标准、安全和服务管理办法（试行）》，该办法对各部分的监管职责予以明确，但划分仍然略显笼统。

为了使监管更加有针对性，笔者认为有必要进一步细化监管实体的组织结构，设置专门的监管机构，以加强对健康医疗数据共享的监管。监管机构的组织结构应融合计算机科学、信息工程、健康医疗以及法律等多领域的专业智慧，以确保其在处理健康医疗数据共享和保护问题时具备全面的评估和应对能力。除了基础的信息安全管理职责，监管机构还需专注于规范信息的二次利用，确保所有的信息共享和利用活动都严格遵守法律规定，同时解决可能出现的个人信息权利和隐私保护方面的问题。通过实施健康医疗信息共享的事前审批或备案制度，监管机制从事前的预防、事中的监督到事后的追责形成了一个完整的闭环，为健康医疗数据共享中的信息安全和个人信息保护提供了有力的保障。

在这个过程中，信息的二次利用规范不仅是对数据安全管理的延伸，也是对法律规定的具体执行，其涵盖了健康医疗数据共享和使用的法律许可范围，以及个人信息权利和隐私保护的核心问题。此类全程监管机制的构建，为医疗信息共享过程中的信息安全和个人信息保护提供了有力的保障，展现一个从多领域专业组合到具体执行机制的完整逻辑链条。

参考文献

[1]胡瑶琳,余东雷,王健.“健康中国”背景下的健康医疗大数据发展[J].社会科学家,2022(03):79-87.
[2]参见高富平.个人信息处理:我国个人信息保护法的规范对象[J].法商研究,2021,38(02):73-86.DOI:10.16390/j.cnki.issn1672-0393.2021.02.006.
[3]参见刘定基：《个人信息的定义、保护原则与个人信息保护法适用的例外——以监控录像为例（上）》，《月旦法学教室》2012 年第 115 期，第 42－54 页。
[4]参见范海潮,顾理平.探寻平衡之道:隐私保护中知情同意原则的实践困境与修正[J].新闻与传播研究,2021,28(02):70-85+127-128.
[5]参见数据匿名化或难以保护个人隐私[EB/OL].[2022-08-10].http://www.xinhuanet.com/tech/2019-07/24/c_1124790278.htm;研究表明,数据匿名化并保护不了你的隐私[EB/OL].[2022-08-10].
[6]参见田野.大数据时代知情同意原则的困境与出路——以生物资料库的个人信息保护为例[J].法制与社会发展,2018,24(06):111-136.
[7]同上。