DOI: 10.16781/j.CN31-2187/R.20250363

· 专题报道 ·

全球视野下医疗人工智能中患者隐私和数据安全：焦点与策略

莫琳芳[1]，李　喆[1]，甘辉亮[1*]，李　立[2*]，王岳杨[1]，张慧杰[1]
1. 海军军医大学（第二军医大学）海军特色医学中心，上海 200433
2. 中山大学附属第一医院《中国神经精神疾病杂志》编辑部，广州 510080

［**摘要**］ 大数据时代下，人工智能（AI）技术发展迅速，医疗领域是其深入应用的领域之一。发挥大数据和AI优势需共享整合医疗数据，但平衡隐私保护和数据共享是重大挑战。本文从数据主权与跨境流动的合规性、患者隐私与数据泄露风险、知情同意与患者自主权的挑战、算法“黑箱”与数据滥用的监管问题、技术依赖与供应链安全风险、隐私保护与公共健康利益的平衡困境6个方面，分析了全球视野下医疗AI中患者隐私和数据安全的焦点问题，并提出应对策略。

［**关键词**］ 人工智能；医疗；隐私安全；数据安全；医学伦理
［**引用本文**］ 莫琳芳，李喆，甘辉亮，等. 全球视野下医疗人工智能中患者隐私和数据安全：焦点与策略[J]. 海军军医大学学报，2025，46（8）：989-999. DOI: 10.16781/j.CN31-2187/R.20250363.

Patient privacy and data security in medical artificial intelligence from a global perspective: focus and strategies

MO Linfang[1], LI Zhe[1], GAN Huiliang[1*], LI Li[2*], WANG Yueyang[1], ZHANG Huijie[1]
1. Naval Medical Center, Naval Medical University (Second Military Medical University), Shanghai 200433, China
2. Editorial Office of *Chinese Journal of Nervous and Mental Diseases*, The First Affiliated Hospital of Sun Yat-sen University, Guangzhou 510080, Guangdong, China

［**Abstract**］ In the era of big data, artificial intelligence (AI) technology has developed rapidly, with medical field being one of its most deeply penetrated application domains. Leveraging the advantages of big data and AI requires the sharing and integration of medical data, yet balancing privacy protection and data sharing poses significant challenges. This paper analyzes the focus issues of patient privacy and data security in medical AI from a global perspective across 6 dimensions: challenges in data sovereignty and cross-border flow compliance, technical vulnerabilities in de-anonymization and re-identification risks, failure of informed consent mechanisms and dynamic authorization needs, regulatory gaps in algorithmic “black boxes” and data misuse, technological dependency and supply chain security risks, and the dilemma of balancing privacy protection with public health interests. Corresponding solutions and strategies are also proposed.

［**Key words**］ artificial intelligence; medical care; privacy security; data security; medical ethics
［**Citation**］ MO L, LI Z, GAN H, et al. Patient privacy and data security in medical artificial intelligence from a global perspective: focus and strategies[J]. Acad J Naval Med Univ, 2025, 46(8): 989-999. DOI: 10.16781/j.CN31-2187/R.20250363.

人工智能（artificial intelligence，AI）作为一门新兴的技术科学，专注于研究和开发用于模拟、延伸及扩展人类智能的理论、方法、技术及应用系统。伴随大数据时代的到来，AI技术得以迅猛发展，医疗领域成为AI应用最为深入的领域之一[1]。AI可对采集到的医学数据进行整合与分析，深度挖掘数据内部蕴含的信息，进而提升医疗决策的准确性与效率，为患者提供更为优质的医疗服务。AI在医学影像分析、辅助诊断与治疗决策、药物研发与精准用药等医疗领域的应用日益广泛，彰显出巨大的潜力。然而，在享受AI带来便利的同时，患者隐私保护和数据安全问题日益凸显，成为制约医疗AI发展的重要因素之一[2]。充分发挥大数据和AI的优势，需对不同来源的医疗数据进行共享和整合。过度强调隐私保护会限制数据的共享与利用，而过度强调数据共享则可能损害患者隐私，如何平

［**收稿日期**］ 2025-06-09　［**接受日期**］ 2025-07-03
［**基金项目**］ 上海市高校科技期刊研究基金（SHGX2024A04），2025年“长江文库计划”编辑学项目（CESSP-CJWK-2025014）. Supported by Research Fund for Shanghai University Science and Technology Journals (SHGX2024A04) and Editorial Project of “The Changjiang Library Plan” in 2025 (CESSP-CJWK-2025014).
［**作者简介**］ 莫琳芳，副研究员. E-mail: molinfang@126.com
*通信作者（Corresponding authors）. E-mail: 2227582941@qq.com, zgsjjs@foxmail.com

衡两者的关系成为一项重大挑战。本文从数据主权与跨境流动的合规性、患者隐私与数据泄露风险、知情同意与患者自主权的挑战、算法“黑箱”与数据滥用的监管问题、技术依赖与供应链安全风险、隐私保护与公共健康利益的平衡困境这 6 个方面，剖析全球视野下医疗 AI 中患者隐私和数据安全的焦点问题，并提出解决策略，以期有效保障患者隐私和数据安全，实现医疗 AI 的可持续发展。

1　数据主权与跨境流动的合规性

数据主权源于国家主权理论，强调国家对境内数据的管辖权，包括立法、司法和行政权力。随着大数据时代的到来，数据已经成为继土地、劳动力、资本、技术之后的第五大生产要素[3]，其价值在于流动，只有动态的数据流汇聚而成的大数据才能充分体现数据的经济价值，释放数字经济的活力[4]。数据跨境流动推动了全球数字经济的发展和创新，其治理水平已成为衡量一个国家综合实力的重要参考标准之一，也是未来大国战略博弈的要点之一[5-6]。

1.1　焦点

1.1.1　*国际层面*　医疗数据跨境共享受到各国法律法规差异和分歧的制约。1995 年，欧洲议会通过《关于个人数据处理中个人权利保护及促进数据自由流通的指令》，简称《95 指令》[7]。随着互联网时代的到来，《95 指令》已无法有效保障个人数据权利和安全。在此背景下，欧盟于 2018 年出台了《通用数据保护条例》（*General Data Protection Regulation*，GDPR），这是全球最严格的个人数据保护法规之一。欧盟依据 GDPR，通过“充分性认定”机制来判断某个国家和地区是否提供了足够的数据保护，决定是否允许数据自由传输，从而限制数据流向保护水平不足的国家，体现其对公民隐私权的优先保护[8]。目前全球仅有部分国家和地区通过了欧盟的“充分性认定”，如安道尔、阿根廷、加拿大等[9]。未通过认定的国家与欧盟国家之间进行医疗数据跨境传输时，需要满足更严格的条件和程序。这种高标准与许多国家的宽松政策形成冲突。美国主要通过行业自律和市场驱动管理数据流动，1986 年生效的《存储通信法案》（*Stored Communication Act*，SCA）没有明确美国政府的搜查令是否能要求通信服务商提交存储在境外的数据[10]。例如，2013 年纽约南部地区法院发布了一项允许政府向微软公司获取其存储的用户电子邮件内容与元数据的搜查令，要求其提供存储在爱尔兰服务器上的用户电子邮件数据，微软公司拒绝配合，理由是数据存储地在爱尔兰，不属于美国管辖范围[11]。这一案件引发了关于数据主权和跨境数据调取的广泛争议，也催生了 2018 年美国《澄清域外合法使用数据法案》（*the Clarifying Lawful Overseas Use of Data Act*，CLOUD 法案）的出台[12]。CLOUD 法案授权美国与符合条件的国家签订双边数据共享协议，允许调取境外数据，为解决此类案件提供了一个突破口。

1.1.2　*国内层面*　中国已构建以《个人信息保护法》[13]、《网络安全法》[14]、《数据安全法》[15]为基础的数据跨境制度体系，明确了数据出境需通过安全评估、标准合同、保护认证 3 种路径[16]。（1）安全评估：适用于重要数据（如涉及国家安全或公共利益的医疗数据）和大规模个人信息（如超过 100 万条非敏感或 1 万条敏感信息）的出境，需经国家网信部门审批。（2）标准合同：针对中小规模个人信息（如临床试验受试者数据）出境，需签订标准化合同并备案。（3）保护认证：通过第三方机构认证，简化跨国公司内部数据传输流程。依据安全评估、标准合同和保护认证要求，医疗数据要求在境内存储，但其适用范围存在重叠和空白。例如，非个人且非重要的医疗数据（如医疗器械供应链数据）缺乏明确跨境规则，形成了监管真空。现有制度缺乏统一的数据主权理论指导，实践过程中有时过度强调安全，而跨国药企和 AI 研发机构常需国际数据协作，导致企业因合规成本高昂而暂停跨境业务。

1.2　应对策略

1.2.1　*国际层面*　（1）推动建立统一的国际规则和标准：各国政府应积极参与国际数据治理合作，通过多边或双边协商，共同制定统一的医疗数据跨境共享规则和标准，明确数据保护的基本原则、跨境传输的条件、数据主体的权利义务等内容，减少因各国法律差异而导致的冲突和不确定性，为医疗数据的跨境流动创造更加稳定、透明和可预期的环境。（2）签订双边或多边合作协议：与其他国家签订专门的医疗数据跨境共享合作协议，就数据流动的具体条件、监管机制、执法合作等达成共识，

建立常态化的沟通协调机制，及时解决数据跨境过程中出现的问题和争议。如 WHO 框架下的《全球数字健康契约》，建立了医疗数据跨境流动白名单机制，允许符合隐私标准的机构参与数据交换[17]。欧盟与美国之间曾尝试通过《安全港协议》《隐私盾协议》等方式探索跨大西洋的数据流动合作模式，尽管这些协议存在一定的局限性，但为国际数据合作提供了有益的经验借鉴[18]。（3）加强司法协助与执法合作：各国司法机关和执法部门应加强在跨境医疗数据执法领域的合作，建立高效的司法协助机制，共同打击数据跨境传输中的违法犯罪行为，如数据泄露、数据窃取、非法跨境数据交易等。通过司法协助与执法合作，能够有效维护数据安全和患者的合法权益，增强各国对跨境数据流动的信任和信心。

1.2.2　国内层面　（1）优化数据出境安全管理机制：借鉴国际上先进的数据出境管理经验，进一步完善国内的数据出境安全评估制度，明确评估的标准、程序和责任主体，提高评估的科学性、公正性和效率[19]。同时，建立健全数据出境后的持续监督机制，确保数据出境活动的全程可控，及时发现并纠正潜在的数据安全风险。（2）合理确定数据本地化存储要求：在保障国家数据安全和监管需求的前提下，根据不同类型医疗数据的风险等级，合理确定数据本地化存储的范围和条件，避免过度本地化对医疗数据的跨境共享和国际合作造成不必要的阻碍。对于一些非敏感或低敏感的医疗数据，可以适当放宽本地化存储限制，允许其在符合条件下跨境传输。试点“数据海关”制度，如海南博鳌医疗旅游先行区[20]，在安全评估后允许特定数据出境。（3）加强数据保护监管力度：强化国内数据保护监管机构的职责和权力，加强对医疗数据的保护和监管。

2　患者隐私与数据泄露风险

在大数据时代，数据量庞大且分散在多个数据源中。数据融合技术可将来自不同渠道、不同格式的数据进行整合，使得原本单独存在的匿名化数据更容易与其他数据结合，增加了再识别的可能性。攻击者可利用数据融合技术将匿名化数据与公开的数据源（如人口普查数据、社交媒体数据等）进行关联分析，通过比对数据中的共同特征，如性别、年龄、地域、职业等间接标识符，重新识别出个体身份。

2.1　焦点

2.1.1　国际层面　20 世纪最著名的用户隐私泄漏事件发生在美国马萨诸塞州，该州团体保险委员会（Group Insurance Committee，GIC）公布了雇员的住院治疗记录以供公共医学研究，为了防止用户隐私泄露，删除了姓名、地址、社会安全号等标识信息，但保留了邮政编码、出生日期和性别。来自麻省理工学院的 Sweeney 通过将这些信息与人口普查数据结合，成功识别出了包括州长在内的多名患者的具体身份和健康状况[21]。2019 年，保加利亚 DSK 银行发生一起 3 万多份客户信息（包括核心生物识别数据）泄露事件，最终该银行被监管机构依照 GDPR 处以 51.5 万欧元的罚款[22]。2025 年 3 月，美国基因检测公司 23andMe 宣布申请破产，美国加利福尼亚州总检察长 Rob Bonta 警告称该公司的财务困境可能对消费者基因数据隐私构成风险。即使该公司声称未经用户同意，不会与医疗保险公司、雇主或公共数据库共享信息，但第三方可能通过分析匿名化数据的模式重新识别出用户身份[23]。

2.1.2　国内层面　中国医疗机构数据脱敏标准不一，导致数据泄露事件频发。2020 年，成都一名 20 岁新型冠状病毒感染（coronavirus disease 2019，COVID-19）女孩的活动轨迹被公开，其真实姓名、身份证号码、住址等隐私信息被公布在网上，致使其遭受网络暴力[24]。广西一名医护人员利用工作之便，非法下载 8.9 万多条新生儿和产妇的个人信息，并将其转卖给外部人员，非法获利[25]。这些案例凸显了中国医疗机构在数据脱敏处理及患者隐私保护方面存在的问题，亟须加强信息管理和技术防护，完善相关制度与标准，以保障患者隐私安全。

2.2　应对策略

2.2.1　管理层面　建立国家级医疗数据脱敏标准，借鉴美国《健康保险携带和责任法案》“安全港”规则，对医疗数据进行全面分类分级，并根据数据的敏感程度和隐私风险确定不同的脱敏要求和管理措施[26]。对身份识别信息（如姓名、地址、出生日期、电话号码等）应严格限制，明确在医疗数据脱敏过程中必须去除的具体信息项，确保这些信息无法被直接或间接地用于识别个体身份。制定统一的数据

脱敏流程，包括数据采集、存储、传输、共享等各个环节的脱敏操作规范，明确各环节的责任主体和操作要求，确保数据隐私在全生命周期中的安全性。

2.2.2　技术层面　采用技术手段处理数据，保留特征，去除可识别信息，进行数据脱敏。（1）k- 匿名模型：其基本原理是确保每个包含标识符属性值相同的等价类至少包含 k 个记录，这样攻击者无法将个体与其他个体有效区分，从而无法确定某个个体的具体信息[27]。在医疗数据中，可将患者的年龄、性别、地域等信息进行分组，使每个分组中至少包含 k 个患者。（2）差分隐私：通过向数据中加入适当的噪声来实现隐私保护。例如，在医疗机构发布患者数据时，可添加一定范围的随机噪声，使攻击者难以获取个体的真实数据[28]。（3）数据替换：使用与原始数据具有相同特征结构的虚拟数据替换原始数据。这样能有效保护数据主体隐私，同时为数据挖掘和机器学习等应用提供丰富替代方案。

3　知情同意与患者自主权的挑战

3.1　焦点

3.1.1　国际层面　欧盟 GDPR 要求“明确同意”，对不同场景下用户同意的信息获取和使用进行了细化规定，明确告知义务只需涵盖与用户决策相关的信息，而不必包括与用户决策无关的其他信息；在取得用户同意的场景下，仅需告知数据处理者对个人信息的使用目的，无须为后续受托者对信息的处理目的单独取得用户同意。虽然 GDPR 在用户同意的可操作性方面做了积极倡导，强化了构成有效用户同意的标准，但其最大局限在于未认识到知情同意机制本身存在严重的局限性，患者常被迫接受宽泛条款，如“未来所有研究使用”，实质上违背了自主权[29]。

3.1.2　国内层面　《个人信息保护法》[13]规定了处理个人信息应当取得个人同意，以及在何种情况下个人信息处理者可以处理个人信息的例外情形。但是在实际工作过程中，医院常通过格式条款一次性获取授权，且格式条款往往内容复杂、专业术语多，患者难以充分理解其中关于个人信息处理的具体内容和后果，无法在充分知情的前提下自愿、明确地作出同意表示，患者也无法追溯或撤回数据，如 AI 模型训练后的数据删除。

3.2　应对策略

3.2.1　制度设计　随着技术的不断进步和人们对隐私保护意识的提高，推行“动态同意”（dynamic consent）平台，允许患者通过 APP 实时调整数据使用范围，这种方案在医疗领域具有显著的优势和潜力，能够增强患者自主权、提高数据质量和相关性、促进研究和创新，有助于推动医疗技术的创新和发展，加速新药物、新疗法的研发和应用。例如，牛津大学研究人员参与的英国健康宝——NHS COVID-19，是英国国家医疗服务体系（National Health Service，NHS）开发的一款自愿使用的手机应用程序，旨在帮助监测和控制 COVID-19 疫情在英格兰和威尔士的传播，该应用程序采用了匿名代码和蓝牙技术追踪接触者，所有数据经过加密处理且 14 d 后自动删除[30]。患者可通过 APP 选择是否共享特定数据（如诊断记录、用药信息），并实时调整共享范围（如仅允许研究机构访问匿名数据，或限制特定时间段的数据使用）。类似技术可迁移至医疗 APP 中，确保患者数据不被直接关联到个人身份。

3.2.2　技术赋能　采用区块链技术记录医疗数据授权链，可有效确保患者对数据流向的可验证性，并通过智能合约实现授权的灵活撤回。区块链的加密技术和不可篡改特性，确保医疗数据在存储和传输中的安全性，防止数据泄露和未授权访问[31]。患者掌握数据访问和使用的控制权，能根据自身需求灵活调整授权范围，更好地保护隐私。区块链自动记录授权链，减少人工管理成本和错误，加快数据共享和停止速度，提升医疗数据管理效率。其中，爱沙尼亚的电子健康档案系统是区块链技术在医疗数据管理中应用的成功典范[32]。该系统为每位公民创建独特数字身份，使其能访问和控制个人健康数据；区块链确保数据不可篡改和安全存储，授权医疗人员安全访问和更新数据，患者亦能追踪数据访问情况。这不仅能够保护患者隐私，还提升了医疗效率和质量，为全球医疗数据管理做出了表率。

4　算法“黑箱”与数据滥用的监管问题

算法被视为复杂且神秘的系统，除设计者和使用者外，他人难以知晓其如何将输入转化为输出。随着算法的复杂性和多样性不断增加，其不可知性也有所上升，这给监管带来了极大挑战。当前，监

管机构往往因缺乏对算法技术的深入了解而难以对其进行有效监管，无法准确判断算法是否存在偏差、不公平等问题。算法“黑箱”问题不仅涉及技术层面，还涉及法律层面。目前，对于算法解释权的具体内容尚未形成统一标准，相关法律规定不够明确和细致，难以对算法“黑箱”进行有效的法律规制。

4.1　焦点

4.1.1　国际层面　AI 模型可能利用患者数据开发非医疗衍生品，超出原始授权范围。2015 年，谷歌的 AI 公司 DeepMind 与 NHS 信托签署合作协议，开发 Streams 应用程序，用于实时分析患者健康数据以帮助医护人员识别急性肾损伤[33]。然而，约 160 万例患者的个人记录在缺乏明确同意的情况下被共享给 DeepMind。2022 年，英国律师事务所代表 160 万例患者提起集体诉讼，指控 DeepMind 未经授权获取并处理医疗记录[34]。英国信息专员办公室（Information Commissioner’s Office，ICO）裁定该数据共享协议违反多项数据保护原则，包括透明度、数据最小化使用、主体性及安全性原则。尽管 DeepMind 修改了协议并新增数据收集和审查规定，但争议持续并最终导致诉讼。该案例提示监管机构应当在数据伦理方面坚持严格原则，确保患者数据仅用于医疗目的，防止滥用。

4.1.2　国内层面　当前国内医疗数据的监管机制尚不完善，部分医院与 AI 企业的合作缺乏透明度和规范性。一些 AI 企业以提供医疗信息化系统为条件，要求医院共享患者数据用于模型训练，但未在合作协议中明确数据使用边界。例如，某三甲医院与企业签订协议时，仅约定“数据用于科研”，但企业后续将数据转售给保险机构用于风险评估，构成违规[35]。此外，监管机构对数据二次使用的监管存在缺失，导致数据滥用问题难以被及时发现和纠正。现行法规未明确数据二次使用的定义及监管主体。医院将患者数据提供给企业用于模型训练后，企业将数据与其他来源数据结合分析，可能重新识别患者身份，但监管机构难以追溯责任[35]。这种合作模式可能导致患者数据被用于超出原始授权范围的商业目的，缺乏透明度和患者知情同意。部分 AI 企业与医院合作开发 AI 医疗产品时，虽然声称仅使用去标识化数据，但实际操作中可能存在数据泄露或滥用风险。

4.2　应对策略

4.2.1　法律约束　《个人信息保护法》[13]、《数据安全法》[14]、《网络安全法》[15]均明确医疗数据处理需遵循“合法、正当、必要”原则，但未细化操作规范，可借鉴 GDPR 完善相关法律，制定“医疗数据保护条例”，强制要求医疗 AI 符合“目的限定”原则，明确数据二次使用的定义、授权流程及违规处罚标准。要求医疗 AI 的数据处理者在收集患者数据前，必须明确、具体且合法地说明数据处理的目的，并确保后续的数据使用与这些目的相符。积极推进算法审查制度，要求医疗 AI 企业在算法投入运营前，向监管部门提交算法产品的准入审查申请，包括算法的原理、数据使用情况、潜在风险及应对措施等。监管部门进行形式和内容上的实质性审查，对于通过审查的算法产品，核发电子牌照，并建立全国联网的牌照系统，以便后续查询、监管与问责。要求医疗 AI 企业在向医疗机构或患者提供服务时，必须履行算法解释义务，清晰地说明算法的原理、数据来源、处理方式及可能存在的风险等，确保患者和医疗机构能够充分了解算法的运作机制。

4.2.2　技术监管　建立严格的数据访问控制机制，仅允许授权人员在必要范围内访问患者数据，部署数据使用监控系统，应用自动化审计工具，对数据访问行为进行记录和审计，实时审计跟踪 AI 模型输入输出，确保数据未被超范围调用，防止数据泄露和滥用。通过数据质量检查、模型性能评估、公平性检测和可解释性分析，实现 AI 系统全生命周期的合规性审查。区块链技术凭借其去中心化、不可篡改、可追溯的特性[31]实现算法审计全程追溯，在破解算法“黑箱”与防范数据滥用方面展现出独特价值。细化去标识化技术规范，采用联邦学习、安全多方计算、双重差分隐私等技术对患者数据进行加密处理，使得数据在二次使用中不可识别，实现“数据可用不可见”，确保数据在存储和传输过程中的安全性，即使数据发生泄露，未经授权的第三方也难以获取其中的真实信息。

5　技术依赖与供应链安全风险

5.1　焦点

5.1.1　国际层面　医疗 AI 的核心技术，如大模型训练框架、高性能芯片、底层算法库，多由少数国

家或企业主导。Futurum Intelligence 在 2024 年 8 月发布的分析报告中明确指出，2023 年英伟达占据全球 AI 图形处理器（graphics processing unit，GPU）市场 92% 的份额[36]。目前以谷歌、Meta、亚马逊、微软等代表的互联网科技公司凭借自身的数据、技术和资本等优势持续在 AI 框架生态领域发力，引领全球 AI 框架技术创新升级趋势，并逐步形成了以 Google-TensorFlow 和 Meta-PyTorch 为代表的双寡头格局[37]。这种集中化导致下游应用方在模型训练、算力支撑等环节缺乏自主可控能力，一旦遭遇技术封锁或断供，会直接引起医疗 AI 系统的研发与运行瘫痪。医疗 AI 的供应链涉及数据标注、硬件组件（传感器、服务器）、软件模块等多个环节，高度全球化。例如，医疗影像标注可能依赖其他国家外包团队，芯片制造依赖特定国家的晶圆厂。这种分散性使其易受地缘政治、贸易摩擦影响，如关键组件禁运、数据跨境传输限制等，可能导致供应链断裂或成本激增。

5.1.2　国内层面　医疗 AI 底层框架被美国企业垄断，存在断供风险。2019 年 5 月 16 日，美国商务部将华为及其 70 个附属公司列入出口管制的“实体清单”，要求美国企业必须经过美国政府批准才可以和华为交易[38]。2022 年，美国对我国实施新的芯片出口管制措施，壁仞科技和摩尔线程等国内芯片研发企业被列入“实体清单”。国内企业难以获取先进的 GPU 芯片，而神经网络模型的训练需要通用性较高的 GPU 进行，这使得我国医疗 AI 相关企业的研发和业务发展受到阻碍，延缓了相关技术的创新和应用。医疗机构依赖进口医疗设备内置 AI 系统，患者数据可能经境外服务器中转，违反了数据本地化要求。我国医疗影像设备市场长期被国外跨国公司如 GE、飞利浦、西门子等垄断，这些企业在影像设备原始数据接口等方面形成了数据生态的“护城河”，国内医疗机构在使用相关设备及配套 AI 系统时，数据的获取、存储和使用等环节存在被“卡脖子”的风险[39]。一旦国外供应商因故实施技术封锁或断供，可能导致国内医疗机构的进口医疗设备无法正常运行，相关 AI 辅助诊断等功能失效，影响医疗诊断和治疗工作的开展，且此前积累的大量患者数据可能面临丢失或无法有效利用的情况。

5.2　应对策略

5.2.1　突破核心技术，实现自主可控　医疗 AI 领域的“自主可控”核心目标是摆脱对外部技术的单点依赖，掌控核心技术迭代主动权。医疗 AI 的技术依赖主要集中在算力层（芯片）、框架层（训练工具）、算法层（专用模型）、数据层（安全处理）4 个核心环节，国产替代需在每个环节实现技术闭环。（1）算力层：国产华为昇腾 910B 芯片采用达芬奇架构，支持混合精度计算，已用于联影医疗的 PET-CT AI 分析系统。华为昇腾 CloudMatrix 384 超节点的部分性能甚至超过英伟达产品[40]。（2）框架层：国产框架需在兼容性、易用性、医疗场景优化 3 个方面进行突破，防范国外框架的代码依赖、升级受限、潜在“后门”等风险。（3）算法层：其自主可控需摆脱对国外预训练模型的依赖，建立国产算法的“精度－泛化性－可解释性”优势。（4）数据层：医疗数据具有高敏感性，其处理技术（如数据脱敏、跨院协同）的自主可控是医疗 AI 系统“自主可控”的前提，避免依赖国外隐私数据计算工具。例如，华为 MindSpore 采用联邦学习和差分隐私技术保障数据安全，用于医疗 AI 领域可提升 AI 诊断能力，保护患者数据隐私[41]。百度的飞桨 PaddlePaddle 提供从底层深度学习框架、深度学习服务平台到产业级模型库的全流程开发支持，降低 AI 开发门槛，在医疗影像识别、疾病预测、药物研发等场景中具有广泛应用价值[42]。国内的科研机构和企业可以联合起来共同打造一个开放、共享的医疗 AI 技术平台，通过开源社区及共享医疗 AI 相关数据、模型、算法等资源降低研发成本，提高研发效率，推动医疗 AI 技术的快速发展和应用创新。华为昇思 MindSpore 开源框架已孵化、支持 50 多个国内外主流大模型，2024 年报道其开源版本累计获得 1 100 万次下载，覆盖全球 130 多个国家和地区的 2 400 多个城市，有 3.7 万多名开发者参与社区贡献[43]。

5.2.2　供应链审查全链透明、安全认证、动态监控　（1）数据供应链全链路审计：建立数据流转台账，记录数据采集、清洗、标注、训练的全流程节点与经手方，通过区块链等技术实现数据溯源，避免数据被篡改或恶意注入，管控敏感信息风险。（2）硬件与软件供应链采取安全准入：医疗 AI 设备（如 AI 辅助诊断仪、智能监护设备）的硬件供应链（如芯片、传感器、主板）可能存在“后门”或质量缺陷。需对硬件供应商实施分级管理，

并在生产环节引入第三方检测，排查潜在“后门”或故障风险。医疗 AI 的软件供应链包括操作系统、数据库、中间件、AI 模型模块等，需对第三方软件供应商进行安全评估，优先选择通过医疗级安全认证的组件。（3）强化风险隔离与应急响应：医疗 AI 进入临床前需模拟供应链攻击场景进行压力测试，验证系统的容错性与恢复能力。医疗 AI 常依赖云服务、第三方应用程序编程接口，需与服务提供商签订安全协议，明确数据加密传输、访问权限管控、漏洞响应时效等责任。

6　隐私保护与公共健康利益的平衡困境

我国虽有多部法律对隐私权和个人信息保护作出规定，但仍存在法律适用的模糊地带，导致在处理隐私保护与公共健康利益冲突时难以准确平衡两者关系。随着大数据、云计算、AI 等技术的发展，个人信息的收集、传输和存储更加便捷和高效，这为公共健康领域的疾病监测、流行病学研究、疫情防控等工作提供了有力支持。然而，也增加了信息泄露和滥用的风险，一旦这些数据被不当使用或泄露，将对个人隐私造成严重损害。

6.1　焦点

6.1.1　*国际层面*　COVID-19 疫情期间各国推行接触者追踪 APP，但过度采集位置数据引发隐私争议。挪威数据保护局于 2020 年 7 月 7 日发布正式声明，指出 Smittestopp 实时上传 GPS 坐标至中央服务器构成对用户位置的持续性监控，存在数据泄露风险，且缺乏数据最小化设计，下载量未达预期（仅占人口 14%），导致隐私侵犯与实际效益失衡，因此对其实施临时禁令[44]。巴林的 BeAware Bahrain、科威特的 Shlonik 和卡塔尔的 EHTERAZ APP 实时跟踪用户 GPS 位置数据并上传至中央服务器，还要求用户绑定国家身份证号码，甚至需佩戴蓝牙手环以确保用户不远离手机[45]。这种过度收集和集中存储数据的方式使用户隐私面临被滥用和泄露的风险。

6.1.2　*国内层面*　中国的健康码 APP 在 COVID-19 疫情防控中发挥了重要作用，但也存在隐私泄露和数据透明度问题。2022 年，《人民日报社民生周刊》报道，河南部分村镇银行储户被强行赋红码，健康码被用于非疫情防控目的，暴露了健康码数据被滥用的风险，引发了公众对其隐私权被侵犯的担忧[46]。2023 年，北京速跑软件公司因未对“人类基因外显子数据分析系统”采取技术防护措施，导致 19.1 GB 基因数据暴露于互联网，违反《数据安全法》被罚款 5 万元[47]。基因数据包含个体遗传特征，一旦泄露可能引发保险歧视、就业歧视等社会问题，同时影响公共健康研究的数据质量。

6.2　应对策略

6.2.1　*伦理权衡*　2023 年 12 月，国际标准化组织 / 国际电工委员会（International Organization for Standardization/International Electrotechnical Commission，ISO/IEC）发布了《人工智能伦理治理体系要求》[48]的国际标准。医疗 AI 伦理困境的解决不是牺牲一方成全另一方，而是通过清晰的伦理原则划定边界、多元参与凝聚共识、全流程审查防控风险，最终实现个体隐私有尊严、公共健康有保障的伦理平衡。（1）确立适配医疗 AI 的核心伦理框架。传统医学伦理的“尊重自主、不伤害、行善、公正”原则需结合医疗 AI 的技术特性升级。①分级伦理优先级原则：日常场景以尊重个体自主为核心，隐私保护优先于非必要的公共健康数据利用。紧急场景启动公共健康优先的伦理原则例外，但需满足“最小必要、限时使用、事后追溯”三大伦理约束，避免例外常态化侵蚀个体隐私。②可解释性伦理原则：医疗 AI 算法的“黑箱”特性可能导致隐私数据被滥用时难以追溯。需要求算法对数据的收集、处理、共享逻辑进行可解释性说明，让个体理解其数据如何被用于公共健康，同时便于伦理审查与公众监督。（2）构建利益相关方的伦理共识。由政府主导，吸纳患者代表、伦理学家、医护人员、AI 企业人员、公共卫生专家共同组成医疗 AI 伦理委员会，针对具体场景制定伦理指南。突破传统单向知情同意局限性，采用动态知情同意模式，允许患者根据自身意愿选择数据使用范围。（3）嵌入全流程伦理审查。建立覆盖“数据收集－算法训练－应用落地－数据销毁”全生命周期的伦理审查机制。

6.2.2　*技术折衷*　技术解决办法的核心逻辑是将个体隐私信息与公共健康所需的群体特征数据分离，通过技术方式，让数据在不暴露个体隐私的前提下释放其在公共健康中的群体分析价值。（1）联邦学习：将 AI 模型的训练过程分布式部署在各医疗机构，各机构仅上传模型参数至中心服务

器，中心服务器聚合参数更新全局模型，再将优化后的模型下发至各机构迭代。整个过程中，原始医疗数据始终存储在本地，不发生跨机构传输，避免原始数据集中存储导致的风险。（2）差分隐私技术：在流行病学模型中引入差分隐私技术，通过在数据发布或共享前添加适当的噪声确保个体数据的隐私性得到保护，使得攻击者难以从输出结果中推断出个体的具体信息，同时保持数据的整体统计特性[28]。（3）同态加密：对原始数据进行加密后，允许直接在加密数据上进行计算，并确保计算结果解密后与原始数据计算结果一致。数据在存储、传输、计算的全流程中始终处于加密状态，只有授权方能解密最终结果。加密数据可安全跨机构共享。（4）动态数据脱敏与分级授权：根据数据使用场景的隐私敏感度和公共健康需求进行分级授权，动态性调整数据脱敏级别并通过技术手段严格管控访问权限。

7　医疗 AI 数据系统性治理体系的构建

为全方位应对医疗 AI 隐私与数据安全的严峻挑战，亟须构建医疗 AI 数据“制度－技术－管理”三位一体系统性治理体系，推动医疗 AI 行业健康、有序发展，在保障患者隐私的前提下释放医疗 AI 的临床价值。见图 1。

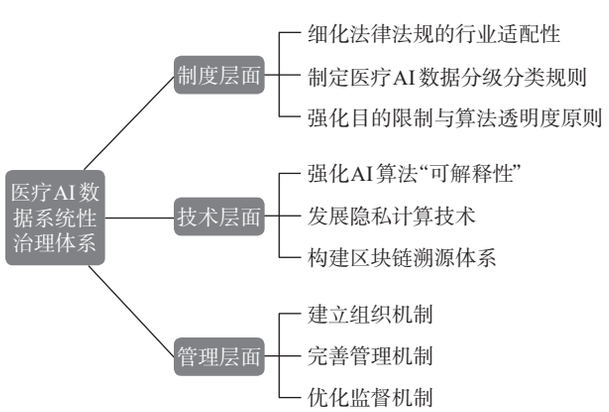

图 1　医疗人工智能（AI）数据系统性治理体系

7.1　*制度层面*　建议以《全球数据安全倡议》[49]为基础，国际协同立法与国内专项法规互补。制定全球医疗 AI 数据公约，统一数据保护标准，明确跨国数据流动规则，促进医疗 AI 技术国际合作，助力全球公共卫生事业发展。目前中国医疗数据安全管理缺乏专项法规，应进一步制定和完善法规体系，明确数据处理各环节的法律责任，提供具体操作指引，以保障医疗数据安全和患者隐私。

7.1.1　*细化法律法规的行业适配性*　国外经验对我国数据安全制度的完善有积极意义，但绝不意味着全盘照搬，在参考时应审慎借鉴，着重考察问题得到良好解决效果的处理方案，最终服务于完善我国的监管规则。在数据跨境、数据本地化、执法调取跨境数据等多个问题上提出我国实质性立场。可以在我国数据监管领域的基础性法规（如《个人信息保护法》《网络安全法》《数据安全法》）[13-15]修订和具体监管细则出台之际，全面融入我国在数据监管领域的战略主张，并通过顶层设计界定医疗 AI 数据流转中的权利、义务与禁止性规范，使其最终服务于我国的国家利益。

7.1.2　*制定医疗 AI 数据分级分类规则*　参考《数据安全法》[15]的重要数据分级思路，将医疗 AI 数据分为 3 级。一级数据（核心隐私数据）如基因、艾滋病史等，仅允许在经个体单独同意和公共健康紧急必要双重条件下使用，且需全程加密；二级数据（敏感健康数据）如慢性病记录、用药史等，可在隐私计算技术保护下用于科研或 AI 模型训练，但需个人授权和机构备案；三级数据（非敏感聚合数据）如体检资料等一般性数据，在去标识化后可用于公共卫生决策，无需个人授权但需明确来源和脱敏标准。

7.1.3　*强化目的限制与算法透明度原则*　通过行政法规明确要求医疗 AI 开发者在产品设计阶段即明确数据使用目的，并通过技术手段锁定用途。制定算法相关法律和制度，着重强调算法技术本身的公开透明性，要求相关主体公开算法的运算数据、源代码及相关决定的输入与输出过程，以此提升算法透明度，进而实现对数据的监管[11]。

7.2　*技术层面*　医疗 AI 应用场景复杂，涉及多模态数据融合、跨机构协同及高敏感数据处理，传统单一加密、权限隔离的安全防护技术难以抵御新型攻击[19]。因此，需通过构建主动防御＋动态适配的先进技术体系实现数据“完全可解释”“可用不可见”“可控可追溯”，从而在不暴露原始数据的前提下支撑数据的安全共享与深度分析，从源头减少隐私泄露与滥用风险。

7.2.1　*强化 AI 算法“可解释性”*　欧盟 GDPR 要求医疗 AI 必须具备“完全可解释性”，国内可借鉴这一标准，禁止不可解释的“黑箱”算法用于关键

诊疗场景。医疗 AI 算法需从技术层面向用户公开“数据使用逻辑”，从而避免因算法“黑箱”导致用户对数据使用的不信任。

7.2.2　发展隐私计算技术　单一技术难以应对复杂场景，针对医疗 AI 数据共享中的核心矛盾，根据场景特性选择适配的隐私计算技术，并不断发展新技术，通过技术组合和发展形成全方位防护[48]。（1）联邦学习：可联合训练多家医院的 AI 模型，但各自数据不离开本地服务器，仅共享模型参数；（2）差分隐私技术：可在公共健康统计中加入噪声数据，既保证统计趋势准确，又无法反推个体信息；（3）同态加密：允许 AI 在加密数据上直接运算，确保运算结果解密后仍准确。

7.2.3　构建区块链溯源体系　基于区块链技术[31]建立“医疗 AI 数据护照”，确保医疗 AI 数据的采集、传输、使用全流程上链，记录操作主体、时间、目的、流转轨迹。个人可通过区块链存证授权记录，若发生数据滥用通过区块链即可快速追溯责任方。

7.3　管理层面　从管理层面看，医疗 AI 数据治理的核心是通过组织架构设计、权责机制划分、流程标准化、利益协调与风险共担破解多主体分散化治理的低效性与责任模糊性，形成目标一致、权责清晰、流程闭环、动态适配的协同共治管理网络[50]。

7.3.1　建立组织机制　构建多元参与、分层负责的协同治理组织架构机制。明确谁来管、管什么、向谁负责的问题，需建立跨主体、分层级的组织体系，避免多头管理或责任真空。顶层决策层构建国家级 / 省级协同治理委员会，负责制定国家级医疗 AI 数据治理战略、审定核心标准、协调跨区域 / 跨部门重大争议；执行协调层构建机构级数据治理联盟，落地顶层战略、搭建区域数据共享平台、解决日常协同问题；操作执行层构建主体内部治理单元，对医疗 AI 研究进行隐私风险评估、伦理与合规双重审查。

7.3.2　完善管理机制　建立全流程闭环、权责清晰的核心管理机制。围绕数据全生命周期（采集→处理→共享→应用→销毁）设计标准化流程，明确各主体的权责，确保每一步操作有规可依、有人负责。（1）数据采集：由顶层委员会制定标准“动态知情同意”模板，明确数据用途、保留期限、共享范围；医疗和研究机构需将患者或研究对象授权信息上传至联盟区块链平台备案，确保授权可追溯。（2）数据处理：使用经联盟认证的脱敏工具，对核心敏感数据采用加密＋差分隐私双重处理，处理后的数据需经第三方机构核验。（3）数据共享：实施白名单＋智能合约制度，仅联盟认证的主体可接入共享平台；共享时需触发智能合约，自动记录用途、时长，超范围使用时平台自动阻断。（4）数据应用：AI 模型上线前需通过多中心临床验证；应用中嵌入风险仪表盘，实时监测算法偏见、隐私泄露风险，触发阈值时自动暂停服务。

7.3.3　优化监督机制　构建内外兼顾、全程可溯的监督网络。通过内部自查和外部监督、多层级管理协作，共同守护数据安全，确保管理机制落地，避免有规不依、违规不究。（1）内部自查：AI 企业定期开展隐私影响评估，重点检查模型训练数据的来源合规性、加密措施有效性；医疗、科研机构设立医疗 AI 数据伦理审查委员会，成员应包括法学专家、医学专家、隐私保护学者、数据科学家、患者代表、公众代表和信息安全专员等，对医疗 AI 的数据使用方案进行伦理评估和审查。（2）外部监督：建立医疗 AI 数据合规审计强制制度，要求医疗 AI 产品必须通过第三方机构的合规审计，重点审查数据采集是否符合“最小必要”、数据存储是否采用加密技术、数据共享是否获得必要授权等。国家卫生健康委员会、网信办等监管部门定期和不定期进行检查。同时，倡导公众监督。患者可通过政务 APP 查询自己的数据使用记录，对可疑记录发起投诉；设立“吹哨人制度”，举报违规使用数据情况。

8　小　结

当前，全球医疗 AI 中的患者隐私与数据安全治理正在数据主权与跨境流动、患者隐私与数据泄露、知情同意与患者自主权、算法“黑箱”与数据滥用、技术依赖与供应链安全、隐私保护与公共健康利益的多重角力中寻找平衡。本文构建的医疗 AI 数据“制度－技术－管理”三位一体系统性治理体系通过制度约束与原则建立，设立了医疗 AI 数据分级分类规则，明确跨国数据流动规则；通过强化标准和技术赋能保证了数据安全，让 AI 真正服务于精准医疗与公共健康；通过监督管理和权责划分守护了隐私保护与伦理底线，保障医疗 AI 以人为本，实现可持续发展；有助于医疗 AI 在安全可控的前提下惠及人类健康福祉。

［参 考 文 献］

［1］ HAMET P, TREMBLAY J. Artificial intelligence in medicine[J]. Metabolism, 2017, 69S: S36-S40. DOI: 10.1016/j.metabol.2017.01.011.

［2］ 杨力，桑祖喜，陈凌敏. 基于数据治理的违规统方管理策略研究[J]. 电子元器件与信息技术，2021，5(10)：229-230. DOI: 10.19772/j.cnki.2096-4455.2021.10.105.

［3］ 李菲. 大数据时代带来的“数据财富”[J]. 浙江经济，2013(17)：16-17. DOI: 10.3969/j.issn.1005-1635.2013.17.011.

［4］ 叶传星，闫文光. 论中国数据跨境制度的现状、问题与纾困路径[J]. 北京航空航天大学学报(社会科学版)，2024，37(1)：57-71. DOI: 10.13766/j.bhsk.1008-2204.2023.2035.

［5］ 李静，卓柳俊，闫文光，等. 医院医学临床研究中健康医疗数据出境现状研究[J]. 中国数字医学，2024，19(8)：108-112. DOI: 10.3969/j.issn.1673-7571.2024.08.018.

［6］ 易永豪，唐俐. 我国跨境数据流动法律规制的现状、困境与未来进路[J]. 海南大学学报(人文社会科学版)，2022，40(6)：135-147. DOI: 10.15886/j.cnki.hnus.202111.0418.

［7］ Directive 95/EC of the European Parliament and of the Council of on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The European Parliament and the Council of the European Union[J]. Stud Health Technol Inform, 1996, 27: 83-118.

［8］ 胡海浪. 论欧盟《通用数据保护条例》的域外效力[J]. 盐城工学院学报(社会科学版)，2024，37(2)：25-29. DOI: 10.16018/j.cnki.cn32-1499/c.202402006.

［9］ 张衡. 跨境数据流动的国际形势和中国路径[J]. 信息安全与通信保密，2018，16(12)：21-26. DOI: 10.3969/j.issn.1009-8054.2018.12.005.

［10］ 田旭. 美国《云法案》对跨境司法机制的新发展[J]. 海关与经贸研究，2018，39(4)：89-101. DOI: 10.3969/j.issn.1674-1765.2018.04.010.

［11］ 魏求月. 数据跨境调取的审查规则构建：《数据安全法》第 36 条重塑[J]. 法律适用，2023(6)：55-67.

［12］ 洪延青. 美国快速通过CLOUD法案 明确数据主权战略[J]. 中国信息安全，2018(4)：33-35. DOI: 10.3969/j.issn.1674-7844.2018.04.017.

［13］ 中华人民共和国个人信息保护法[EB/OL].(2023-09-10)[2025-06-01]. *https://www.mca.gov.cn/zt/n2717/n2719/c1662004999979994833/content.html.*

［14］ 中华人民共和国网络安全法[EB/OL].(2023-09-10)[2025-06-01]. *https://www.mca.gov.cn/zt/n2717/n2719/c1662004999979994833/content.html.*

［15］ 中华人民共和国数据安全法[EB/OL].(2023-09-10)[2025-06-01]. *https://www.mca.gov.cn/zt/n2717/n2719/c1662004999979994833/content.html.*

［16］ 孙志煜，洪一帆. 数据跨境“白名单”制度的理论阐释与规则构建[J]. 杭州电子科技大学学报(社会科学版)，2025，21(3)：41-50. DOI: 10.13954/j.cnki.hduss.2025.03.004.

［17］ GWAGWA A, MOLLEMA W J T. How could the United Nations Global Digital Compact prevent cultural imposition and hermeneutical injustice?[J]. Patterns (N Y), 2024, 5(11): 101078. DOI: 10.1016/j.patter.2024.101078.

［18］ 钟鸣. 数字贸易时代个人信息跨境流动的法律保护路径[J]. 人民论坛•学术前沿，2021(6)：108-111. DOI: 10.16619/j.cnki.rmltxsqy.2021.06.013.

［19］ 许皖秀，左晓栋. 全球竞争格局下的中国特色数据跨境流动治理方案研究[J]. 中国工程科学，2025，27(1)：111-121. DOI: 10.15302/J-SSCAE-2024.12.007.

［20］ 赵亮亮. 医疗变革先行者：海南博鳌医疗旅游先行区[J]. 西部皮革，2018，40(13)：113. DOI: 10.3969/j.issn.1671-1602.2018.13.067.

［21］ 大数据环境下的隐私保护技术[EB/OL].(2015-06-01)[2025-06-01]. *https://www.cac.gov.cn/2015-06/01/c_1115473995.htm.*

［22］ Bulgaria: CPDP issues penal order of BGN 1M to DSK Bank[EB/OL].(2019-08-28)[2025-06-01]. *https://www.dataguidance.com/news/bulgaria-cpdp-issues-penal-order-bgn-1m-dsk-bank.*

［23］ 李木子. 23andMe宣布破产基因数据前途未卜[N]. 中国科学报，2025-03-28(1).

［24］ 成都确诊女孩遭网暴背后：信息泄露违法成本低，维权成本高[EB/OL].(2020-12-10)[2025-06-01]. *https://www.163.com/dy/article/FTFTNGAV05129QAF.html.*

［25］ 广西一医护人员倒卖 8 万条婴儿信息被追责 前例源头多为内鬼[EB/OL].(2020-09-29)[2025-06-01]. *https://www.toutiao.com/article/6877850233439519245/?upstream_biz=doubao&source=m_redirect.*

［26］ 曾益康. 数据时代健康信息交换中的隐私保护：以美国《HIPAA 法案》为例[J]. 中国数字医学，2022，17(3)：6-10. DOI: 10.3969/j.issn.1673-7571.2022.3.002.

［27］ SWEENEY L. k-Anonymity: a model for protecting privacy[J]. Int J Uncertain Fuzziness Knowl Based Syst, 2002(10): 557-570. DOI:10.1142/S0218488502001648.

［28］ DANKAR F K, EMAM K E. Practicing differential privacy in health care: a review[J]. Trans Data Privacy, 2013, 6(1): 35-67.

［29］ 范为. 大数据时代个人信息保护的路径重构[J]. 环球法律评论，2016，38(5)：92-115. DOI: 10.3969/j.issn.1009-6728.2016.05.007.

［30］ WYMANT C, FERRETTI L, TSALLIS D, et al. The epidemiological impact of the NHS COVID-19 app[J]. Nature, 2021, 594(7863): 408-412. DOI: 10.1038/s41586-021-03606-z.

［31］ 冯涛，焦滢，方君丽，等. 基于联盟区块链的医疗健康数据安全模型[J]. 计算机科学，2020，47(4)：305-311. DOI: 10.11896/jsjkx.190300087.

［32］ Estonia’s leadership in blockchain-based electronic health records[EB/OL].(2023-08-23)[2025-06-01]. *https://sites.uw.edu/theston/2023/08/23/estonias-leadership-in-blockchain-based-electronic-health-records/*.

［33］ SUBHAJIT B, AUDREY G. Restoring trust into the NHS: promoting data protection as an ‘architecture of custody’ for the sharing of data in direct care[J]. Int J Law Inf Technol, 2020, 28(3): 243-272. DOI: 10.1093/ijlit/eaaa014.

［34］ LOVELL T. Google and DeepMind face legal claim for unauthorised use of NHS medical records. The data on 1.6 million patients was allegedly used without their consent[N/OL]. Healthcare IT News, 2022-05-17[2025-06-01]. *https://www.healthcareitnews.com/news/emea/google-and-deepmind-face-legal-claim-unauthorised-use-nhs-medical-records.*

［35］ 张汉成. 健康医疗数据共享的现实困境与合规因应[J]. 医学与哲学，2024，45(17)：52-57. DOI: 10.12014/j.issn.1002-0772.2024.17.11.

［36］ Futurum Intelligence releases AI chipset market share analysis, 5-year forecast, revealing vendor revenue and growth[EB/OL].(2024-08-19)[2025-06-01]. *https://www.01net.it/futurum-intelligence-releases-ai-chipset-market-share-analysis-5-year-forecast-revealing-vendor-revenue-and-growth/*.

［37］ 2023 年美国AI框架行业市场现状及竞争格局分析Google、Meta双寡头格局[EB/OL].(2023-08-16)[2025-06-01]. *https://bg.qianzhan.com/report/detail/300/230816-4cafec90.html.*

［38］ 任志宽. 华为全球供应链分析与风险评估[J]. 广东科技，2019，28(11)：58-61. DOI: 10.3969/j.issn.1006-5423.2019.11.017.

［39］ 刘盼盼，钟永恒，刘佳，等. 专利视角下中国“卡脖子”企业现状分析及突破建议[J]. 科技管理研究，2024，44(16)：162-172. DOI: 10.3969/j.issn.1000-7695.2024.16.018.

［40］ 昇腾破局 国产算力不再低调[EB/OL].(2025-06-23)[2025-07-01]. *https://baijiahao.baidu.com/s?id=1835723942109442601&wfr=spider&for=pc*.

［41］ 付稚柳. 基于MindSpore平台的联邦蒸馏系统设计与实现[D]. 北京：中国科学院大学，2022.

［42］ 张心怡. 百度飞桨：AI深度学习技术自立自强，加速产业智能化升级[J]. 大数据时代，2022(11)：26-37.

［43］ 昇思开源四年，开放生态如何引领中国AI框架突围？[EB/OL].(2024-12-17)[2025-06-01]. *https://m.163.com/dy/article/JJKJQUJO0534A4SC.html?referFrom=*.

［44］ Norway: data protection authority upholds prior prohibition on collection of data via COVID-19 App Smittestopp[EB/OL].(2020-07-13)[2025-06-01]. *https://www.loc.gov/item/global-legal-monitor/2020-07-13/norway-data-protection-authority-upholds-prior-prohibition-on-collection-of-data-via-covid-19-app-smittestopp.*

［45］ cnBeta. 报道称海湾国家将COVID-19接触者追踪App作为大规模监控工具[EB/OL].(2020-06-17)[2025-06-01]. *https://tech.sina.com.cn/roll/2020-06-17/doc-iirczymk7425489.shtml.*

［46］ 维权储户被强行赋红码？乱动的手别滥用！“一码归一码”[EB/OL].(2022-06-15)[2025-06-01]. *https://www.toutiao.com/article/7109313650485101056/?upstream_biz=doubao&source=m_redirect.*

［47］ 未采取技术防护措施致基因数据暴露在网络上，北京速跑软件公司被罚5万[EB/OL].(2022-07-05)[2025-06-01]. *https://c.m.163.com/news/a/I8TJ94EF0514R9KQ.html.*

［48］ ISO/IEC. Information technology—artificial intelligence—management system: ISO/IEC 42001:2023[S/OL]. Geneva: International Organization for Standardization, 2023.[2025-06-01]. *https://www.iso.org/standard/42001.*

［49］ 中方提出《全球数据安全倡议》[J]. 中国信息安全，2020(9)：8-9.

［50］ 吴腾. 生成式人工智能技术赋能智慧医疗建设的风险与规制[J]. 医学与社会，2025，38(3)：9-16. DOI: 10.13723/j.yxysh.2025.03.002.

［本文编辑］ 孙　岩