网络化医疗中的大规模隐私保护

M. Amin
Rahimian匹兹堡大学工业工程系美国宾夕法尼亚州匹兹堡
rahimian@pitt.edu

Benjamin Panny匹兹堡大学智能系统项目美国宾夕法尼亚州匹兹堡
bmp83@pitt.edu

James B.D.Joshi匹兹堡大学信息学与网络化系统美国宾夕法尼亚州匹兹堡 jjoshi@pitt.edu

arXiv:2601.04298v1 [cs.CR] 7 Jan 2026

摘要——**数字化、网络化医疗有望实现更早检测、精准治疗和持续护理；然而，这也扩大了隐私泄露和合规风险的暴露面。我们主张从孤立、针对特定应用的保护措施，转向**大规模隐私保护设计，**其核心包括：贯穿整个医疗数据生命周期的决策论差分隐私（DP）；针对人员、传感器和组织之间相互依存关系的网络感知隐私核算；以及**代码化合规**工具，使卫生系统能够共享证据，同时证明其履行了监管尽职义务。我们综合梳理医疗领域的隐私增强技术（PET）格局（联邦分析、差分隐私、密码计算），指出实践中的不足，并提出可部署的行动方案，包括隐私预算台账、用于协调不同站点隐私增强技术组件的控制平面、共享测试平台以及隐私增强技术素养，从而使合法、可信的共享成为默认做法。我们通过多个应用场景（多中心试验、基因组学、疾病监测、移动健康）加以说明，并强调**分布式推理**是明确设定隐私预算下开展多机构学习的核心方法。**

索引词——**差分隐私、联邦学习、隐私增强技术、健康数据共享、代码化合规、分布式推理**

I. 联网医疗保健中的隐私未来

医疗保健的核心职能依赖于医疗服务提供者与患者之间的信任；如果患者隐私遭到侵犯，这种信任就会受到损害 [1]。维护强有力的隐私保证，也有助于保护患者数据，避免其被滥用于牟利、勒索、歧视性做法等。随着数字化医疗数据和数据驱动的计算框架迅猛增长，数据将在未来的医疗人工智能中发挥核心作用，并有望提升质量、降低医疗保健成本。然而，这种以数据为中心的未来带来了确保患者隐私方面的新挑战，因此需要建立基础性的隐私框架，以便将其统一应用于医疗保健系统的不同组成部分。

健康数据日益丰富，加之机器学习和人工智能不断进步，为重塑健康科学和医学开辟了重要机遇[2]。数据驱动的计算框架已渗透到健康科学和医学的各个领域，从数字接触者追踪 [3], [4] 、促进心理健康与心理健康福祉 [5] ，到医学图像分析 [6]、癌症诊断 [7], [8], 、糖尿病视网膜病变识别 [9]、心律失常检测 [10], 、外科手术 [11], 和创伤护理 [12]。智慧与数字健康[13], [14] 和精准医学 [15], 等主要医疗保健趋势，以及人工智能驱动的行为改变等新兴理念，有望改善健康结果，并借助数字技术实现个性化且普惠的医疗服务提供。这些技术以高分辨率生物特征数据（例如心率、呼吸频率、血压和血氧水平）、生物医学数据（例如基因组学和蛋白质组学），以及生活方式和环境测量数据（例如通过可穿戴传感器采集）为基础，并结合人工智能赋能的分析，用于检测、分类、诊断和护理优化。要实现这些积极的社会成果，取决于患者是否信任医疗服务提供者并愿意与其分享数字健康数据 [16], [17]。

健康相关数据被视为敏感数据（例如，根据《通用数据保护条例》第 9 [18] 条），需要受到特别保护，因为此类数据一旦泄露，可能侵犯基本权利和个人自由，使人们在就业、保险和服务方面遭受各种形式的歧视，也可能导致滥用或攻击。患者与医疗服务提供者之间的信息共享对于医疗保健职能至关重要，并受到职业保密原则的保护（其根源可追溯至《希波克拉底誓言》）。然而，随着医疗保健系统日益复杂，数字医疗数据迅猛增长并广泛应用于医疗保健运营的各个方面，我们亟需采取整体性方法来降低隐私风险，并在公共卫生和改善医疗服务带来的社会效益与个人所面临的风险之间取得平衡。

《健康保险可携性与责任法案》(HIPAA)、《遗传信息非歧视法》(GINA)以及《联邦人类受试者保护政策》（《共同规则》）等法规相继出台，旨在规范数据治理，并缓解与健康数据相关的隐私问题。然而，数字健康领域瞬息万变，医疗保健领域的信息规范又具有情境性，因此需要灵活、充分且适应性强的框架，以全面评估新兴技术带来的隐私与效用之间的权衡 [19]，贯穿整个医疗保健周期，并覆盖支撑公共卫生协议和医疗服务提供的数据收集及算法流程。在描绘可规模化医疗保健隐私的愿景时，我们一方面着眼于广泛共享数据的必要性，以最大限度地发挥其在医学进步和健康科学中的作用，并支持数据驱动的干预措施日益广泛地应用于整个医疗保健周期以及公共卫生协议中的筛查、诊断、预后、治疗和监测；另一方面，也着眼于平衡

监测和控制疾病、改善医疗保健并推动健康科学发展的社会效益，与个人享有的隐私、尊严和自决权，以及免受因共享健康数据而产生的偏见和歧视所造成的不当伤害的权利。

A. 与国家优先事项和战略举措保持一致

在医疗保健场景及其他领域私密地共享和分析数据的能力，与《关于安全、可靠和值得信赖地开发和使用人工智能的行政命令》相一致。该命令强调隐私增强技术（PETs）在负责任人工智能未来中的作用 [20]，也与早前的《推进隐私保护型数据共享与分析的国家战略》相一致。该战略呼吁协调推进一系列隐私增强技术、试点项目、标准、测试平台、可用性、劳动力发展和国际合作，以“以肯定民主价值观的方式，增进个人和社会的福祉与繁荣，并促进科学与创新” [21]。

其他联邦路线图进一步明确了研究界的这一议程：《国家隐私研究战略》优先开展跨学科工作，以降低数据分析和人工智能带来的隐私风险，并推进机器可读政策和问责制 [22]；《联邦网络安全研发战略计划》强调整合身份、访问、互操作和可衡量的隐私风险最小化的信任模型 [23]；*NIST*人工智能风险管理框架和《人工智能权利法案蓝图》着重关注处理敏感数据的人工智能系统所涉及的以人为本的透明度、安全性和公平性问题 [24], [25]；而*NIST*隐私框架则提供了企业风险管理视角，用于评估数据生命周期各环节的隐私、安全和效用权衡 [26]。这些战略为研究界勾勒出一份路线图：对隐私增强技术进行端到端评估和基准测试，建立兼顾政策的数据和模型生命周期，将可用性和透明度融入设计，制定严谨的权衡指标，并建设连接研究、部署与新兴标准的共享测试平台 [21]–[23]。

B. 适应不断演变的监管与政策格局

健康数据使用规则正在发生变化，既为学习型医疗卫生系统提供支持，也对其加以限制。在研究领域，美国国立卫生研究院的数据管理与共享政策（自2023年1月25日起生效）提高了对数据再利用的要求，使隐私保护设计方法和可审计生命周期成为首要需求，而非附加选项 [27], [28]。除《健康保险流通与责任法案》外，美国联邦贸易委员会更新的《健康信息泄露通知规则》明确要求许多消费者健康应用和联网设备履行泄露通知义务，从而加强数字健康生态系统中的问责制；这些生态系统与临床工作流程和社区健康相互联通 [29]–[31]。在临床信息技术领域，美国国家卫生信息技术协调员办公室（ONC）近期颁布的规则（HTI-1）为认证健康信息技术中的预测性决策支持增加了透明度和安全性方面的义务，使模型生命周期可审计成为实际要求，并加强信息共享 [32], [33]。

在网络规模层面，《可信交换框架与共同协议》（TEFCA）是美国的一项国家级倡议，旨在根据《21世纪治愈法案》的要求，促进不同健康信息网络（HINs）之间安全、无缝且覆盖全国的电子健康信息（EHI）交换。TEFCA指定的合格健康信息网络（QHINs）及候选网络正在逐步完善全国范围的交换渠道，拓展了通过合规即代码（隐私预算台账、数据溯源、机器可读政策）履行应有审慎义务、同时促进跨机构学习的空间 [34]。与此同时，2025年的一项诉讼裁决撤销了美国卫生与公众服务部（HHS）于2024年对《健康保险流通与责任法案》作出的生殖健康隐私修订，这凸显了围绕受保护健康信息（PHI）合法流动的跨司法管辖区不确定性，以及可移植隐私保证的重要性 [35]–[37]。

在国际层面，欧盟人工智能法案（《欧盟官方公报》2024年7月12日）将许多医疗保健人工智能应用归类为“高风险”，并要求进行全生命周期风险管理、履行透明度义务，这将影响跨大西洋合作；与此同时，《通用数据保护条例》对二次使用和跨境传输的限制仍在持续影响临床研究 [38], [39]。与此同时，新兴的生物识别规则（例如，加强告知与同意要求、保留期限限制，以及若干州的私人执法）进一步强化了这一方向，鼓励采用尽量减少原始信号保留、并将敏感特征保留在边缘端的设计：加利福尼亚州依据《加州消费者隐私法》/《加州隐私权法》，将生物特征数据视为“敏感个人信息”；华盛顿州通过《我的健康、我的数据法》纳入了生物识别符法；伊利诺伊州于2024年修订了《生物识别信息隐私法》（BIPA），同时保留私人执法权；而得克萨斯州针对大型平台执行生物识别法律所达成的创纪录和解协议，也进一步印证了这些趋势 [40]–[45]。在联邦层面，美国联邦贸易委员会的生物识别政策声明阐述了针对模型训练和部署中不公平使用的理论依据（包括未能评估可预见危害、算法偏见和测试不足，以及暗中或出乎意料的数据收集、未经监控的数据管道和未经审查的第三方使用）；目前的提案，例如《美国隐私权法案》讨论稿和《2025年旅行者隐私保护法案》，则表明未来可能建立国家基准，使可移植的、由隐私增强技术支持的分析成为务实的默认选择 [46]–[48]。

在第 II 节中，我们将探讨能够推动隐私增强技术在个性化和数字化医疗保健领域应用的基础理论。结合第 III 节中有助于提升用户体验并促进合规的工程设计，这些基础理论将帮助我们逐步建立一个以健康数据隐私为核心的实践共同体。在第 IV 节中，我们将探讨一些应用案例，说明负责任人工智能领域的发展如何对医疗保健产生重大影响，并提高人们对隐私增强技术和隐私保护分析在健康研究与实践中重要性的认识和重视，从而促进监管合规与伦理合规。最后，我们将在第 V 节中总结全文，并介绍理论与工程进步最能发挥影响力的机遇和挑战。

II. 网络医疗中的可扩展隐私基础

现实世界中的健康数据具有相互依存性：患者共享家庭和社区；医疗服务提供者在团队中协作；各机构参与多中心研究；公共卫生行动则沿着接触网络和转诊网络传播。在此类情境中，隐私失误会沿关联传播，而不仅仅是通过记录泄露。因此，保障措施必须保护信息流（暴露信息、邻域统计数据、信念更新），而不能只保护静态表格。

差分隐私（DP）提供了一种稳健的隐私定义，已成为隐私保护分析的黄金标准，能够在保障统计精度和可信度的同时，兼顾个人隐私风险。传统的匿名化、哈希和加密技术往往繁琐、缺乏规范且成本高昂，更适用于可信方之间的数据整理，因为研究表明，这些技术容易受到多种身份识别 [49]，链接攻击和交叉引用攻击 [50]–[52]，伪再识别 [53]，以及统计差异攻击和再识别攻击 [54]；总而言之，它们无法应对数字化和个性化医疗保健带来的隐私挑战。差分隐私对现代隐私研究产生了深远影响，并已应用于政府的大规模、高知名度项目，例如美国十年一次的人口普查 [55] 以及科技行业（例如，跟踪表情符号使用情况的统计数据 [56]，[57]），但差分隐私在医疗保健领域的实用化、大规模实施仍然有限（或许最近发布的以色列国家活产登记处微观数据是个例外 [58]，[59]）。

差分隐私要求，作用于数据的算法（机制）的输出分布几乎不因某个个体记录的存在、缺失或修改而改变，从而限制对手（或任何观察者）通过观察输出对输入所能作出的推断 [60]，[61]。这通常通过在算法设计中引入随机化来实现。例如，随机化方案可以用特定方式向原始数据添加噪声，使对手无法判断原始数据集中是否包含任何特定个体的数据。其隐私形式化保证如下：作用于患者数据 $s \in \mathcal{S}$ 的机制 $\mathcal{M}: \mathcal{S} \to \mathcal{R}$，如果对于任意一对相邻观测 s，s' 以及范围空间 $\mathcal{R}$ 的任意子集 $\mathfrak{R}$，均满足 $\mathbb{P}[\mathcal{M}(s) \in \mathfrak{R}] \leq e^{\varepsilon}\mathbb{P}[\mathcal{M}(s') \in \mathfrak{R}] + \delta$，则称其满足 (ε, δ)-差分隐私。对 $\mathcal{M}$ 的 (ε, δ)-差分隐私约束确保，当 $\varepsilon, \delta \to 0$ 时，无法推断 s 或其任何相邻点是否为生成观测输出 $\mathcal{M}(s)$ 的输入。数据集之间的邻接概念通常定义为相邻数据集仅在某个个体实体的贡献上有所不同，因此 (ε, δ)-差分隐私可保护个体贡献，避免其因对手的推断而受到不利影响。因此，不同的邻接概念会为个体提供不同的保护。这种信息论层面的保证使算法输出即使面对量子计算（或任何计算能力不受限制的对手）带来的威胁，也可以安全发布。参数 ε 称为隐私预算，其中 $\varepsilon \to \infty$ 对应于不提供任何隐私保护的非隐私情形。

当 $\delta = 0$ 时，我们得到纯差分隐私约束（ε-差分隐私），该约束由 $\delta > 0$ 放宽。以医疗保健场景中的一个具体例子来说，考虑一名患有心血管疾病的患者是否参加临床试验：该疾病使患者中风风险比普通人群的 0.01% 高出 2%。如果保险公司得知这一情况，患者的保费将增加 600 美元，以计入中风风险增加 2% 所带来的成本；一次中风将造成 30,000 美元的损失。这可能会令患者不愿参加试验；然而，如果以 ε-差分隐私方式进行分析，且 $\varepsilon = 1$，那么保险公司通过观察试验数据推断出的风险最多只会增加 $0.01(e^1 - 1)\% = 0.017\%$，相当于保费增加 5.1 美元，患者或许能够接受这一增幅。在不同场景下，向输入数据添加噪声有助于落实 (ε, δ)-差分隐私约束，但添加的噪声也可能降低性能，例如降低分布式估计 [62]，[63] 或靶向干预 [64]，[65] 的质量。随之而来的隐私—效用权衡十分复杂，需要对医疗保健场景中的决策流程进行审慎建模。将情境完整性与差分隐私结合起来，可将其作为一种设计视角 [66]，[67]，使技术措施适应临床和公共卫生规范，目标是通过将隐私视为随数据和决策流动的系统属性，而不只是文件的属性，在大规模应用中提供可审计保证。

最新进展。 目前，医疗保健场景中的隐私保护分析方法主要针对特定应用，例如基因组学 [68]、电子健康记录的合成生成 [69]和临床试验数据 [70]，[71]。联邦学习（FL）是一种广受欢迎的机器学习（ML）和人工智能（AI）模型去中心化优化与分布式训练范式[72]，[73]，其基于数据最小化原则，通过免去将所有数据点收集到中央服务器进行梯度计算的需求，来缓解隐私障碍[74]，[75]，在医疗保健预测分析领域也展现出广阔的应用前景 [76]，[77]。尽管联邦学习提供了基本的隐私保护，但由于威胁假设各异，仍存在各种隐私问题，文献中也提出了多种隐私保护联邦学习方法 [78]。差分隐私（DP）是另一种广受欢迎的方法，通过向算法输出中注入受控噪声和随机性来限制隐私泄露 [51]，[79]，，并已成功应用于生物医学数据分析（例如医学影像[80] 和基因组数据隐私 [81]）及数据共享 [82]，[83]，，包括与联邦学习结合使用 [84]，[85]。最后，诸如同态加密、函数加密和多方计算等密码学技术，能够对加密数据进行计算，在医疗保健场景中展现出广阔的应用前景 [86]，[87]；然而，这些方法强大的密码学保障需要以牺牲计算效率为代价，而且其实现受信息技术（IT）要求和计算资源的限制，许多组织和设备无法满足这些要求。可信执行环境，或更广为人知的机密计算，通过基于硬件的信任链，为端到端隐私解决方案提供了更快速的替代方案，并可与其他方法互为补充 [88]–[90]。

目前缺少这样一种框架：它能够灵活、一致地应用于医疗服务提供和公共卫生运营；具有足够的表达能力，使我们能够权衡数据共享对医疗服务消费者及其社区的风险与益处；并且不局限于典型标准，例如在将差分隐私和联邦学习的最新进展应用于医疗保健场景时，对估算统计准确性或人工智能和机器学习模型预测性能的考量。

面向从数据到决策全过程隐私保护的决策理论差分隐私。差分隐私可作为统计披露控制嵌入数据和模型生命周期的各个阶段，使隐私保证与决策——例如试验入组、资源分配和靶向干预——以及危害——例如保险费率上调和污名化——相一致。对于试验，差分隐私可以限制对手从汇总信号中进行推断，同时保留统计功效；对于疾病监测，差分隐私可以稳定风险沟通，同时避免暴露个人信息。这使隐私重新成为一种设计变量，需要与统计功效、公平性、准确性和成本一并优化 [80], [91]。

面向相互依赖数据的网络感知隐私。随着信息在网络中扩散，隐私机制应保护个人及其关系，其敏感度应随网络拓扑（度分布、聚类和路径长度）以及网络化智能体之间的动态变化（序贯学习和反馈）而调整。网络感知隐私保证可支持分布式试验、生物标志物发现和网络干预等应用，同时限制群体层面信息泄露和累积参与风险 [92], [93]。网络感知隐私领域的基础性进展能够应对数据点相互依赖时所产生的挑战，例如社会与生物医学网络中的情形，并提供保护信息流而非静态网络结构中隐私的解决方案，从而支持对动态场景中的隐私与效用进行严谨分析，例如接触者追踪、生物标志物发现、分布式试验和基于网络的干预。

分布式推理是核心工具。许多网络化任务都可归结为分布式证据累积：各站点计算局部统计量，并交换经过隐私处理的信念更新；由此，站点网络便能作出决策（例如，试验中的优效性判断、变点告警）。向对数似然或其他充分统计量中注入差分隐私噪声，可以保护网络所学到的内容不泄露任何参与者的信息，同时保留决策效用。我们将差分隐私分布式推理 （DPDI）称为一种在隐私约束下实现多站点学习和序贯更新的框架 [62]。

III. 构建网络化医疗保健系统中的可扩展隐私

隐私增强技术（PETs）功能强大，但彼此分散。合成电子健康记录（EHRs）有助于信息传播，但需要风险控制以避免泄漏 [69],[94]。联邦学习（FL）可减少集中式聚合，但除非结合形式化隐私保护，否则模型更新会泄漏信息 [95]–[97], , 临床部署也日益将 FL 与差分隐私（DP）结合使用 [84]。密码学技术，例如安全多方计算（MPC）和同态加密（HE），能够保护机密性，但计算开销可能很大；近期系统（例如基于多方同态加密的联邦分析（FAMHE））证明了其用于跨孤岛分析的可行性 [98]。在实践中，部署会混合使用这些工具，但往往缺乏统一的隐私预算或端到端核算。

既有研究已将差分隐私应用于医学影像和电子健康记录预测，在集中式和联邦式环境中构建了具有记录级保证且对任务有用的模型 [80], [99], [100]。这些系统通常假设数据独立同分布，并采用单任务训练等点式解决方案，且通过一次性隐私核算报告效用。尚未充分说明的是：隐私风险如何随重复参与、跨机构协作以及患者或家庭网络中的传播而组合。本节提出设计原则，用于在此类网络化、多机构环境中分配隐私预算并认证泄漏情况。卫生系统持续学习、跨机构交换模型，并在下游重复使用表征；在这些操作中，风险会累积，并可能沿家庭、医疗服务提供者或地理网络扩散。我们将隐私视为一种系统属性，贯穿（i）**数据收集**（边缘设备监测、知情同意、抽样、日志记录）、（ii）**推断**（统计和机器学习建模流程）以及（iii）**行动**（临床、运营和公共卫生决策）。为此，我们设想通过以下工程进展，将“每个模型的差分隐私”转向“贯穿整个学习工作流的差分隐私”：（*i*）明确管理随时间推移及跨站点的隐私预算，（*ii*）提供网络感知保证，以限制群体级和关联级泄漏，以及（*iii*）将可审计组合纳入代码化合规。

数据模型与互操作性。Observational Medical Outcomes Partnership (OMOP)、Observational Health Data Sciences and Informatics (OHDSI) 和国家以患者为中心的临床研究网络 (PCORnet) 通用数据模型（通用数据模型）为医疗保健研究中的可复现分布式分析标准化了架构和词汇表[101], [102]。例如，Artificial Intelligence-Ready and Equitable Atlas for Diabetes Insights (AI-READI) 项目使用 OMOP 通用数据模型处理临床数据，并使用 DICOM格式处理图像，从而构建 AI-READI数据集 [103]。然而，AI-READI 项目为共享目的构建了一个专用平台（fairhub.io），并采用定制的多层“瑞士奶酪式”访问模型来管理隐私风险 [53]。为了安全地扩大规模，我们需要能够与临床数据模型（OMOP/PCORnet）集成并生成可验证的合规证据的隐私增强技术；也就是说，需要能够与这些数据生态系统集成、配备预审计查询并支持数据溯源的隐私增强技术组件，而不是迫使大型研究联盟各自构建定制治理平台 [53]。

代码化合规与隐私增强技术的未来。机器可读的政策、隐私预算台账、数据血缘、访问日志以及自动生成的机构审查委员会/数据使用协议文本，有助于将代码化合规付诸实践。为提升互操作性，可将生存分析等常见统计任务映射为针对通用数据模型的预审计查询 [104],[105] ，并与 OMOP/PCORnet 架构对齐，以支持插件式

采用。NIST隐私框架和人工智能风险管理框架 [24], [26]可为将此类标准化查询整合到组织风险管理框架中提供参考。未来的隐私增强技术可结合联邦分析，使原始数据保留在原处；使用差分隐私来限制更新与发布之间信息流造成的泄漏，并使用安全多方计算/同态加密处理涉及不可信聚合器和跨站点关联的高风险子程序 [98], ，并提供模块化证明，以支持端到端隐私认证。

IV. 用例、测试平台与面向应用的议程指标

A. 多组学与高维生物标志物

基因组学、蛋白质组学及其他高维生物标志物，正在成为学习型医疗卫生系统中的常规数据。大规模人群研究需要采取严格措施，防范成员身份推断和关联攻击。尽管如此，在大规模人群研究中，针对特征选择和模型发布采用差分隐私，并结合访问代理和后处理检查，可以防范成员身份推断和关联攻击 [83], [100],，但全基因组关联研究（GWAS）类场景的规模和粒度会加剧常见的成员身份推断和关联攻击风险，并带来一类较少受到讨论的社会生物医学 溢出效应：关于某个人的数据可能会泄露其亲属、家庭成员或联系人的隐私事实 [68], [106],[107]。随着队列日益多样化，数据也更加自由地在机构间流动，将此类关系视为首要考量至关重要。

如果从一开始就针对 这些现实进行设计，隐私保护会是什么样子？一种可能的做法是，不把生物标志物发现视为单次发布，而是将其视为一个工作流 ，使其中的选择、测试、共享和再利用都纳入治理视野。在这种思路下，差分隐私为逐条记录的披露提供防护措施；联邦加密分析减少不必要的数据汇集；而兼顾政策要求的审计轨迹有助于确保再利用可问责 [61], [108]。尚待解决的问题是，如何将这些要素融为一体，让隐私保护随生物标志物“同行”——贯穿不同站点、时间和下游应用，同时不损害科学效用。

我们认为有几个值得探索的方向：

- **关系感知敏感度**。许多生物标志物任务具有天然的结构（亲缘关系、共同暴露、系统发育）。在界定敏感度时考虑这些结构，有望在保留从业者所关注信号的效用的同时，降低最坏情况下的泄漏风险 [109],[110]。

- **不确定性下的选择**。发现流程经常会对变异、区域或检测面板进行 top-k 选择。采用轻量级的隐私保护选择机制，并辅以简单且可共享的摘要，或许能在透明度与风险之间实现切实可行的平衡[51], [111]。

- **随时间组合的隐私**。卫生系统会持续学习。与其提供一次性的保证，不如通过隐私预算管理和数据溯源，更轻松地理解风险如何在多次迭代和不同机构之间累积[61], [108]。

- **将压力测试作为一种规范**。除了准确性之外，定期检查成员推断、亲缘关系恢复或接触路径推断，也可以成为方法验证的一部分——类似于其他领域中的稳健性检查 [106], [107]。

这些想法都不需要一套庞大的整体解决方案。更现实的近期做法是采用一系列可互操作的实践：在有帮助时加入适度噪声，在适用时使用预审计查询，并清晰记录所采取的措施及其原因。如果能始终如一地采用这些实践，即使数据集、模型和合作不断扩大，也能让基因组学驱动的学习既实用又受到适当约束。

B. 分布式临床试验与多站点学习

像 AI-READI 项目这样的多站点工作，展示了对可扩展隐私框架的需求：这类框架能够在保护敏感人口统计学和临床数据的同时，实现跨机构分析联邦化。该项目正在协调来自三个不同地理站点的数据，并按种族／族裔、性别和糖尿病状态进行三重平衡，以训练“无偏机器学习模型” [103]。采用差分隐私的联邦试验分析能够加快招募、亚组分析和安全性监测，同时提供跨站点可审计性。影像学和病理学研究展示了联邦学习与差分隐私相结合的实用性 [84] ，而加密分析则证明了其在生存分析和全基因组关联研究类任务中的可行性 [98]。

临床试验是生成医学证据和评估干预措施的金标准。在针对新发疾病测试治疗方法时，招募患者参加临床试验颇具挑战，尤其是在疾病罕见和／或严重、且可用药物不多的情况下。一种解决方案是建立一个临床试验中心网络。艾滋病临床试验组（ACTG）网络便是一个成功案例，但建立该网络需要巨额前期投入和集中协调。然而，更普遍地说，隐私方面的考量往往表现为机构和监管层面的障碍，阻碍了这类环境中的数据共享。例如，多中心临床试验通常需要签署大量数据使用协议，从而拖慢甚至阻止合作。差分隐私分布式推理（DPDI）框架通过仅交换经差分隐私净化的信念统计量，在各站点实现隐私保护假设检验和生存分析，减少对复杂数据使用协议的依赖，同时符合《健康保险流通与责任法案》（HIPAA）／《通用数据保护条例》（GDPR）的要求以及站点治理规定[62]。这与 ARPA–H 的推进临床试验准备度（ACTR）愿景相契合，即开展去中心化按需试验，并自动同步电子健康记录（EHR）与病例报告表（CRF）。DPDI 使各站点能够提供可用于分析的统计量，而无需导出原始受保护健康信息，从而支持大规模招募、亚组分析和安全性监测。与重度依赖密码学的隐私增强技术（同态加密／安全多方计算，HE/MPC）相比，后者虽能提供强有力的形式化保证，却往往需要大量信息技术／高性能计算能力以及各站点的专业工程支持；DPDI 则以低得多的计算与编排开销，实现具有竞争力的准确性与隐私权衡 [87],[98]。这也符合新兴的开放科学实践（例如，

AI-READI 对多站点平衡数据集的治理），DPDI 提供了可审计的流程，与医疗保健领域的联邦分析相协调 [53], [78], [99]。

除了固定的试验分析，网络感知差分隐私种子选择还可驱动自适应的站点与参与者选择策略，在尊重隐私预算的同时提升统计效能和亚组覆盖率。在这一框架下，中期分析仅公开隐私化充分统计量（例如差分隐私分数和对数似然增量），而招募与留存策略可在遵守公平性与泄露约束的前提下，优先考虑高价值分层或站点。差分隐私种子选择框架根据部分联系与转介轨迹[64],提供目标选择机制，而差分隐私分布式推断则为序贯监测以及判定治疗组的优效或无效提供保护隐私的证据累积层 [62]。这些组件共同构成闭环数据决策流程，其中 (i) 下一步邀请谁、(ii) 重点关注哪些站点，以及 (iii) 何时因取得成功或无效而停止，均依据形式化隐私预算和可供审计的组合核算进行调整。

C. 公共卫生运营：接触者追踪、疾病监测、定向筛查与预防措施

COVID-19疫情将公共卫生体系推到了公共话语的焦点位置。许多人对非药物干预、接触者追踪、隔离行动和疫苗接种推广仍记忆犹新 [112], [113]。健全的公共卫生系统对于保障国家的健康与安全至关重要。每当出现新发传染病，这一职责便会受到关注（例如20世纪70年代的军团病、20世纪80年代的艾滋病，以及21世纪初的严重急性呼吸综合征及其变异）。即便不在聚光灯下，公共卫生职能在管理地方性疾病方面仍不可或缺，例如每个流感季节的流感，以及美国阿片类药物危机等长期存在的问题。美国两百多年的公共卫生服务历史，留下了许多为民众生命与生计而奋斗的成功事例。消灭天花[114] ，以及总统艾滋病紧急救援计划在预防HIV感染和艾滋病方面取得的成果 [115]，就是近代史上的两个例子。然而，这项面向公众的职能也面临重大挑战。COVID-19疫情期间，民主国家的信息生态系统失灵，导致有关疫苗接种的错误信息广泛传播 [116]–[118] ，并侵蚀了民众、公共卫生机构与科学界之间的信任 [119]，从而削弱了公共卫生本可产生的广泛影响。信任受损这一挑战日益加剧，而人工智能和数据驱动框架在公共卫生领域的作用也不断扩大；它们虽有望大幅提升运营效率，却也可能加剧现有不平等，并使人们对公共卫生体系更加不信任，尤其是在个人隐私受到侵犯，且数字技术在处理民众的生命与生计相关事务时缺乏透明度与问责制的情况下。在这种情形下，危险并不局限于信任侵蚀，还可能以其他形式出现，例如针对公职人员和科学界的骚扰，这一点在反疫苗运动中已有体现 [120], [121]。

暴露通知、哨点部署和疫情检测都是受约束条件下的网络优化问题。网络感知差分隐私结合次模传感器选择等网络优化框架，可以在限制披露风险的同时保持有效性。接触者追踪通常会产生影响力样本，这些样本是部分级联和短接触路径，而非完整网络。利用此类样本来优化哨点监测、目标选择或播种（例如，为稀缺的预防资源选择初始接收者）{...}会产生双重要求：(i) 从部分数据中学习足够的结构，以实现高干预影响；(ii) 保护追踪所揭示的个人及其关系的隐私。近期研究对这一场景进行了形式化，并针对仅有影响力样本可用的情况[64], [65]，提出了使用差分隐私网络信息进行播种 的隐私概念和算法。

差分隐私（DP）有两种部署模式。在中心化差分隐私（*CDP*）中，可信数据管理者可以查看原始接触样本，但只发布随机化种子集合；在本地差分隐私（*LDP*）中，随机化在数据收集时进行，因此聚合器永远看不到未经保护的样本。理论分析和模拟表明，随着隐私预算减少，CDP 的性能会平稳下降，并阐明了实现强 LDP 保证所需的（更高）预算 [64]。这一框架可直接应用于使用暴露前预防（PrEP）开展的艾滋病毒预防：在男男性行为者（MSM）的性接触网络中，为影响力较大的个体播种，能够放大群体层面的效益。基于实证的 ARTnet 网络模型为美国 MSM 提供了真实的度数和混合模式。 [122], 与此同时，卫生经济学研究一贯支持优先针对风险较高的亚群体，从而提升 PrEP 的成本效益 [123], [124]。因此，考虑网络特征的差分隐私目标选择流程能够：(a) 从追踪和监测工作流中提取带噪声且保护隐私的影响力样本；(b) 选择符合个人及关系的形式化隐私预算的目标；以及 (c) 量化运营政策中的隐私—效用权衡（例如目标数量、执行频率和重新确定目标的规则）。除 PrEP 外，同样的方法还适用于其他疫情应对措施（例如暴露通知和哨点部署），以便在严格进行隐私核算的同时实现早期检测或传播抑制。

D. 移动健康（*mHealth*）生态系统

系统综述指出，监管意图与应用实践之间存在差距。隐私保护设计堆栈（差分隐私查询、带安全聚合的联邦学习、数据飞地和密码学技术）加上防篡改日志，有助于使遥测数据与系统级保障及临床医生审查保持一致 [99]。这对于现代研究方案至关重要，例如大规模部署移动健康设备的方案；AI-READI研究便为约4,000名参与者使用了连续监测10天的连续血糖监测仪（CGM）和Garmin身体活动追踪器 [103]。妥善协调隐私增强技术

可以提供移动健康隐私的“操作系统”，以支持对高速流动遥测数据的处理。

V. 结论、机遇与挑战

从持续采集的生物特征数据和可穿戴设备，到多组学和学习型医疗卫生系统，医疗保健正日益变得智能、互联，并且由人工智能赋能。这些进展依赖于诊所、实验室、支付方、供应商和公共卫生机构之间的数据流动，并最终依赖于公众对数据共享不会造成伤害的信任 [125], [126]。治理框架（《通用数据保护条例》、《健康保险流通与责任法案》、GINA 和共同规则）设定了最低标准，而美国国立卫生研究院数据管理与共享政策、NIST隐私框架和人工智能风险管理框架则推动在更强保障措施下实现更广泛的数据使用 [18], [24], [26], [127]——[130]。然而，现代数据使用的速度、粒度和情境依赖性，要求相关框架能够在实际情境中权衡隐私—效用，而不仅仅依赖事后去标识化模式 [1], [50], [52]；随着新的攻击路径日益受到挑战，例如“伪重新识别”，在包含可穿戴设备、心电图或视网膜成像数据的数据集中，即使不需要个人身份信息，也可以锁定独特的个人[53]。

在网络化医疗中实现大规模隐私保护，在实践中面临若干相互关联的挑战：(i) 在各站点、数据集和连续分析之间（包括联邦式环境中）进行严格、端到端的隐私核算与组合 [74]–[131]；(ii) 针对现代攻击和临床机器学习流程的现实威胁模型，确保系统具备稳健性 [132]；(iii) 通过关联电子健康记录、医学图像及其他医疗保健数据模态，在数据异质性下实现数据协调与公平性，同时避免保护措施过度降低少数群体的效用 [69], [80]；(iv) 建立联邦分析的治理、可审计性和数据溯源机制，使技术保障与新兴组织框架保持一致 [24], [26], [27]–[127], [130]；(v) 为自适应研究和流式研究中的同意管理、撤回和机器遗忘提供切实可行的机制 [43], [133], [134]；(vi) 在社会生物医学情境中，将保护范围从个人扩展至家庭、社区和接触网络 [66], [68]；(vii) 在隐私增强技术（包括差分隐私、安全聚合、多方计算、同态加密、可信执行环境和合成数据技术）之间权衡工程取舍，以满足实际工作流中的准确性、延迟和成本约束 [73], [86], [87], [96], [98], [135]；以及 (viii) 通过公共基准和跨站点审计，开展激励相容的数据共享与评估，并使其与机构风险、监管变化和科学价值保持一致 [28], [122]。

为应对这些挑战，我们设想构建工程技术栈，使隐私成为可审计的一等系统属性。例如，设计向导可将隐私法规和政策条款（如二次使用、有限数据集和有时限的保留）转化为流程图、隐私增强技术组合，以及可追溯其依据、符合数据使用协议要求的文本；隐私预算台账则可借助计算器、组合跟踪、按数据集设置的“隐私标签”，以及流水线 API，支持跨项目和站点的治理（可借鉴 Census TopDown 部署在集中分配、跨表组合和公开文档方面的经验 [136]）。分布式推理中的差分隐私原语，可通过隐私化信念更新和假设检验程序，促进机构间的信息共享与学习 [62]。隐私增强技术协调层可提供一个控制平面，组合差分隐私、安全聚合、同态加密和安全多方计算，以落实数据使用目的、接收方和保留期限限制，记录数据溯源，并将可复用的审计材料与绑定到机器可读配置的证明打包 [86], [87], [135]。最后，合规沙箱以及经过策划、取得知情同意的合成测试平台，可提供攻击者模型和红队测试能力，从而针对真实的联网任务生成易于理解的风险证据。例如，可以利用高保真的合成电子健康记录资源，为患者转诊网络或多中心试验设计测试平台 [69]–[94]。总体而言，这些举措与国家层面对于可用工具、集成解决方案以及用于实践中隐私保护型数据共享的测试平台的重视相一致 [137]。在这些方面取得进展，将有助于构建保护隐私并具备学习能力的医疗保健系统，使其符合伦理、公平、可审计，并能在常规护理中部署。

参考文献

[1] S. J. Nass, L. A. Levit, L. O. Gostin 等，《健康信息隐私的价值与重要性》，载于《超越 *HIPAA* 隐私规则：通过研究增强隐私、改善健康》。美国国家科学院出版社，2009年。[2] P. Rajpurkar, E. Chen, O. Banerjee, and E. J. Topol，《健康与医学中的人工智能》，*Nature Medicine*，第28卷第1期，31–38页，2022年。[3] L. Ferretti, C. Wymant, M. Kendall, L. Zhao, A. Nurtay, L. Abeler- D¨orner, M. Parker, D. Bonsall, and C. Fraser，《对 SARS-CoV-2 传播的量化表明，数字接触者追踪有助于控制疫情》，《科学》，第368卷第6491期，页码 eabb6936，2020年。[4] L. Ferretti, C. Wymant, J. Petrie, D. Tsallis, M. Kendall, A. Ledda, F. Di Lauro, A. Fowler, A. Di Francia, J. Panovska-Griffiths 等，《对700万次接触中的 SARS-CoV-2 传播风险进行数字化测量》，*Nature*，第626卷第7997期，145–150页，2024年。[5] H. Li, R. Zhang, Y.-C. Lee, R. E. Kraut, and D. C. Mohr，《基于人工智能的对话代理促进心理健康与福祉的系统综述和荟萃分析》，*NPJ Digital Medicine*，第6卷第1期，页码236，2023年。[6] Y. Yang, H. Zhang, J. W. Gichoya, D. Katabi, and M. Ghassemi，《公平医疗影像人工智能在真实世界泛化方面的局限》，*Nature Medicine*，1–11页，2024年。[7] T. Chanda, K. Hauser, S. Hobelsberger, T.-C. Bucher, C. Nogueira Gar- cia, C. Wies, H. Kittler, P. Tschandl, C. Navarrete-Dechent, S. Podlipnik, E. Chousakos, I. Crnaric, J. Majstorovic, L. Alhajwan, T. Foreman, S. Peternel, S. Sarap, ¨I. ¨ Ozdemir, R. L. Barnhill, M. Llamas-Velasco, G. Poch, S. Korsing, W. Sondermann, F. F. Gellrich, M. V. Heppt, M. Erdmann, S. Haferkamp, K. Drexler, M. Goebeler, B. Schilling, J. S. Utikal, K. Ghoreschi, S. Fr¨ohling, E. Krieghoff-Henning, R. S. Consortium, and T. J. Brinker，《类皮肤科医生的可解释人工智能提升了黑色素瘤诊断的信任度与信心》，《自然·通讯》，第15卷第1期，页码524，2024年。[8] A. Esteva, B. Kuprel, R. A. Novoa, J. Ko, S. M. Swetter, H. M. Blau, and S. Thrun，《利用深度神经网络实现皮肤癌的皮肤科医生级分类》，*Nature*，第542卷第7639期，115–118页，2017年。[9] R. Gargeya and T. Leng，《利用深度学习自动识别糖尿病视网膜病变》，《眼科学》，第124卷，2017年第7期，962–969页。[10] A. Y. Hannun, P. Rajpurkar, M. Haghpanahi, G. H. Tison, C. Bourn, M. P. Turakhia, and A. Y. Ng，《利用深度神经网络，在动态心电图中实现心脏病专家级的心律失常检测与分类》，*Nature Medicine*，第25卷第1期，65–69页，2019年。

[11] F. Chadebecq, L. B. Lovat, and D. Stoyanov, 《人工智能与自动化在内窥镜检查和外科手术中的应用》, Nature Reviews Gastroenterology & Hepatology, 第20卷第3期, 171–182页, 2023年。[12] J. W. Cannon, D. S. Gruen, R. Zamora, N. Brostoff, K. Hurst, J. H. Harn, F. El-Dehaibi, Z. Geng, R. Namas, J. L. Sperry, J. B. Holcomb, B. A. Cotton, J. J. Nam, S. Underwood, M. A. Schreiber, K. K. Chung, A. I. Batchinsky, L. C. Cancio, A. J. Benjamin, E. E. Fox, S. C. Chang, A. P. Cap, and Y. Vodovotz, 《数字孪生数学模型为失血性休克复苏策略的个体化制定提供依据》, Communications Medicine, 第4卷第1期, 页码113, 2024年。[13] P. Prahalad, D. Scheinker, M. Desai, V. Y. Ding, F. K. Bishop, M. Y. Lee, J. Ferstad, D. P. Zaharieva, A. Addala, R. Johari et al., 《为新确诊的1型糖尿病患者公平实施精准数字健康计划, 以管理血糖》, Nature Medicine, 1–9页, 2024年。[14] C. Chen, S. Ding, and J. Wang, 《面向老龄人口的数字健康》, Nature Medicine, 第29卷第7期, 1623–1630页, 2023年。[15] R. Hodson, 《精准医学》, Nature, 第537卷第7619期, S49–S49页, 2016年。[16] M. M. H. Shandhi, K. Singh, N. Janson, P. Ashar, G. Singh, B. Lu, D. S. Hillygus, J. M. Maddocks, and J. P. Dunn, 《智能设备拥有情况及数字健康数据共享可接受度评估》, NPJ Digital Medicine, 第7卷第1期, 页码44, 2024年。[17] A. R. Miller, 《数字健康信息的隐私》, Economics of Privacy, 1077–1093页, 2022年。[18] 欧洲议会和欧盟理事会, 《条例（欧盟）2016/679（通用数据保护条例）》, https://data.europa.eu/eli/reg/2016/679/oj, 2016年。[19] H. Nissenbaum, 《隐私即情境完整性》, 载于 Washington Law Review, 第79卷, 2004年, 页码119。[20] 《关于安全、可靠和值得信赖地开发和使用人工智能的行政命令》, https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/, 2023年10月, 白宫。[21] 国家科学技术委员会隐私增强技术小组委员会, 《推进隐私保护型数据共享与分析国家战略》, https://www.nitrd.gov/pubs/National-Strategy-to-Advance-Privacy-Preserving-Data-Sharing-and-Analytics.pdf, 总统行政办公室, 技术报告, 2023年。[22] 国家科学技术委员会网络与信息技术研究与发展小组委员会, 《国家隐私研究战略》, https://www.nitrd.gov/pubs/National-Privacy-Research-Strategy-2025.pdf, 2025年。[23] ——, 《联邦网络安全研究与发展战略计划》, https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/01/Federal-Cybersecurity-RD-Strategic-Plan-2023.pdf, 2023年。[24] 《NIST人工智能风险管理框架（人工智能风险管理框架1.0）》, https://www.nist.gov/itl/ai-risk-management-framework, 2023年。[25] 白宫科技政策办公室, 《人工智能权利法案蓝图：让自动化系统服务于美国人民》, https://bidenwhitehouse.archives.gov/ostp/ai-bill-of-rights/, 2022年10月。[26] 《NIST隐私框架：通过企业风险管理改善隐私的工具》, https://www.nist.gov/privacy-framework, 2020年。[27] 美国国立卫生研究院, 《NIH最终数据管理与共享政策（NOT-OD-21-013）》, 2020年, 2023年1月25日起生效。[28] ——, 《提醒：NIH数据管理与共享政策于2023年1月25日生效（NOT-OD-23-053）》, 2023年。[29] 美国联邦贸易委员会, 《FTC敲定对健康信息泄露通知规则的修订》, 2024年4月。[30] ——, 《健康信息泄露通知规则——最终规则（2024年4月25日）》, 2024年。[31] ——, 《健康信息泄露通知规则：企业须知（2024年7月更新）》, 2024年。[32] 国家卫生信息技术协调员办公室, 《健康数据、技术与互操作性：认证计划更新、算法透明度与信息共享（HTI–1）——最终规则》, 《联邦公报》, 2024年1月。[33] HIMSS及相关来源, 《HTI–1最终规则：预测性决策支持与信息共享相关资源》, 2024年。[34] RCE / The Sequoia Project, 《指定的合格健康信息网络》, 2025年。

[35] 美国卫生与公众服务部, 民权办公室, 《HIPAA 隐私规则支持生殖健康护理隐私——最终规则情况说明书》, 2025年。[36] Holland & Knight 摘要, 《Purl诉HHS案（德克萨斯北区联邦地区法院, 2025年6月18日）——撤销生殖健康隐私规则的命令》, 2025年。[37] 路透社, 《美国法官宣布拜登保护堕胎隐私的规则无效》, 2025年6月。[38] 欧盟, 《欧盟条例2024/1689——人工智能法案（《官方公报》, 2024年7月12日）》, 2024年。[39] 多区域临床试验中心, 《GDPR和隐私法律对临床研究的影响》, 2024年。[40] 加利福尼亚州立法机关, 《加利福尼亚州民法典》第1798.140条——定义（《加州消费者隐私法》/《加州隐私权法》）, 2018年。[41] 华盛顿州立法机关, 《生物识别标识符, RCW第19.375章》, 2017年。[42] ——, 《华盛顿州我的健康我的数据法案, RCW第19.373章》, 2023年。[43] 伊利诺伊州, 《伊利诺伊州《生物识别信息隐私法》修正案（SB 2979, 2024年8月2日）：按人计算的损害赔偿与电子同意》, 2024年。[44] 德克萨斯州总检察长办公室, 《德州总检察长宣布与Meta就生物识别数据处理实践达成14亿美元和解》, 2024年7月。[45] 美联社, 《谷歌将向德克萨斯州支付14亿美元, 就生物识别和数据隐私问题达成和解》, 2025年5月。[46] 美国联邦贸易委员会, 《委员会关于生物识别信息的政策声明》, 2023年5月。[47] 国际隐私专业人员协会, 《了解《美国隐私权法案》讨论稿中的“敏感受保护数据”》, 2024年6月。[48] 美国国会, 《2025年旅行者隐私保护法案（S.1691）——法案正文》, 2025年5月。[49] M. Barbaro、T. Zeller和S. Hansell, 《AOL搜索用户第4417749号的身份曝光》, 《纽约时报》, 2006年8月, https://www.nytimes.com/2006/08/09/technology/09aol.html。[50] L. Sweeney, 《只有你、你的医生以及许多其他人可能知道》, 《Technology Science》, 第2015092903卷, 2015年, https://techscience.org/a/ 2015092903/。[51] F. McSherry和K. Talwar, 《通过差分隐私进行机制设计》, 载于《第48届IEEE计算机科学基础年会》（FOCS）论文集。IEEE, 2007年, 第94–103页。[52] L. Sweeney, 《将技术与政策结合起来以维护机密性》, 《法律、医学与伦理学杂志》, 第25卷, 第2–3期, 第98–110页, 1997年。[53] S. Hallaj、A. Heinke、F. G. P. Kalaw、N. Gim、M. Blazes、J. Owen、E. Dysinger、E. S. Benton、B. A. Cordier、N. G. Evans、J. Li-Pook-Than、M. P. Snyder、C. Nebeker、L. M. Zangwill、S. L. Baxter、S. McWeeney、C. S. Lee、A. Y. Lee和B. Patel, 《临床研究中的开放数据共享与参与者隐私：人工智能时代的挑战与机遇》, 2025年8月, arXiv:2508.01140 [q-bio]。[54] R. Kumar、J. Novak、B. Pang和A. Tomkins, 《通过基于令牌的哈希对查询日志进行匿名化》, 载于《第16届国际万维网大会》（WWW）论文集。ACM, 2007年, 第629–638页。[55] R. Gong、E. L. Groshen和S. Vadhan, 《利用已知的未知因素：差分隐私与2020年人口普查》, 《哈佛数据科学评论》, 特别专刊2, 2022年。[56] U. Erlingsson, 《借助掷硬币, 以隐私保护方式学习统计数据》, https://security.googleblog.com/2014/10/learning-statistics-with-privacy-aided.html, 2014年10月。[57] 苹果差分隐私团队, 《大规模隐私保护学习》, https: // machinelearning.apple.com/research/learning-with-privacy-at-scale, 2017年。[58] S. Hod和R. Canetti, 《以差分隐私方式发布以色列国家活产登记处的数据》, 载于《2025年IEEE安全与隐私研讨会》（SP）论文集。IEEE, 2025年, 第3912–3930页。[59] S. Hod, 《设计以色列国家活产登记处的试点发布：协调隐私、准确性与可用性》, 载于《USENIX隐私工程实践与尊重会议》（PEPR）, 2023年, https://www.usenix.org/conference/pepr23/presentation/hod。[60] C. Dwork, 《私有数据分析的坚实基础》, 《ACM通讯》, 第54卷, 第1期, 第86–95页, 2011年。[61] C. Dwork和A. Roth, 《差分隐私的算法基础》。Now Publishers, 2014年。[62] M. Papachristou和M. A. Rahimian, 《差分隐私分布式推断》, medRxiv, 2025年3月, 预印本。[63] ——, 《差分隐私分布式估计与学习》, 《IISE Transactions》, 第57卷, 第7期, 第756–772页, 2025年。

[64] Y. Liu、M. A. Rahimian和F. Yu，《使用差分隐私网络信息进行播种》，arXiv，2025年。[65] M. A. Rahimian、F. Yu和C. Hurtado，《用于影响力最大化的差分隐私网络数据收集》，载于《第22届国际自主智能体与多智能体系统会议》（AAMAS 2023）论文集。国际自主智能体与多智能体系统基金会，2023年，第2795–2797页。[66] H. Nissenbaum，《隐私即情境完整性》，《Washington Law Review》，第79卷，第119–158页，2004年。[67] S. Benthall和R. Cummings，《整合差分隐私与情境完整性》，载于《2024年计算机科学与法律研讨会论文集》，2024年，第9–15页。[68] Z. Wan、J. W. Hazel、E. W. Clayton、Y. Vorobeychik、M. Kantarcioglu和B. A. Malin，《基因组数据隐私的社会技术保障措施》，《自然·遗传学评论》，第23卷，第7期，第429–445页，2022年。[69] J. Yoon、M. Mizrahi、N. F. Ghalaty、T. Jarvinen、A. S. Ravi、P. Brune、F. Kong、D. Anderson、G. Lee、A. Meir等，《EHR-safe：生成高保真且保护隐私的合成电子健康记录》，NPJ Digital Medicine，第6卷，第1期，第141页，2023年。[70] J.-N. Eckardt、W. Hahn、C. R¨ollig、S. Stasik、U. Platzbecker、C. M¨uller- Tidow、H. Serve、C. D. Baldus、C. Schliemann、K. Sch¨afer-Eckart等，《利用生成式人工智能，通过合成急性髓系白血病患者模拟临床试验》，NPJ Digital Medicine，第7卷，第1期，第76页，2024年。[71] B. K. Beaulieu-Jones、Z. S. Wu、C. Williams、R. Lee、S. P. Bhavnani、J. B. Byrd和C. S. Greene，《保护隐私的生成式深度神经网络支持临床数据共享》，《循环：心血管质量与结局》，第12卷，第7期，第e005122页，2019年。[72] N. Shi、F. Lai、R. A. Kontar和M. Chowdhury，《联邦学习中的集成模型：提升泛化能力并量化不确定性》，《IEEE自动化科学与工程汇刊》，2023年。[73] X. Yue、R. A. Kontar和A. M. E. Gomez，《联邦数据分析：线性模型研究》，《IISE Transactions》，第56卷，28，2024 1, 16no. pp. – 。[74] B. McMahan和A. Thakurta，《具有形式化差分隐私保证的联邦学习》，Google AI 博客，2022年，https://ai.googl eblog.com。[75] R. A. Kontar、N. Shi、X. Yue、S. Chung、E. Byon、M. Chowdhury、J. Jin、W. Kontar、N. Masoud、M. Nouiehed等，《联邦物联网（IoFT）》，《IEEE Access》，第9卷，第156 071–156 113页，2021年。[76] G. A. Kaissis、M. R. Makowski、D. R¨uckert和R. F. Braren，《医学影像中的安全、隐私保护型联邦机器学习》，《自然·机器智能》，第2卷，第6期，第305–311页，2020年。[77] J. Xu、B. S. Glicksberg、C. Su、P. Walker、J. Bian和F. Wang，《医疗信息学中的联邦学习》，《医疗信息学研究杂志》，第5卷，第1期，第1–19页，2021年。[78] K. Bonawitz、P. Kairouz、B. McMahan和D. Ramage，《联邦学习与隐私》，《ACM通讯》，第65卷，第4期，第90–97页，2022年。[79] T. Zhu、G. Li、W. Zhou和P. S. Yu，《差分隐私数据发布与分析：综述》，《IEEE知识与数据工程汇刊》，第29卷，第8期，第1619–1638页，2017年。[80] A. Ziller、D. Usynin、R. Braren、M. Makowski、D. Rueckert和G. Kaissis，《采用差分隐私的医学影像深度学习》，《科学报告》，第11卷，第1期，第13524页，2021年。[81] A. Halimi、L. Dervishi、E. Ayday、A. Pyrgelis、J. R. Troncoso-Pastoriza、J.-P. Hubaux、X. Jiang和J. Vaidya，《全基因组关联研究中保护隐私且高效的结果验证》，载于《隐私增强技术论文集》。隐私增强技术研讨会，第2022卷，第3期，2022年，第732–753页。[82] A. Yamamoto和T. Shibuya，《GWAS关键统计数据更实用的差分隐私发布》，《生物信息学进展》，第1卷，第1期，第vbab004页，2021年。[83] C. Uhler、A. Slavkovi´c和S. E. Fienberg，《全基因组关联研究中保护隐私的数据共享》，《隐私与保密杂志》，第5卷，第1期，第137–166页，2013年。[84] M. Adnan、S. Kalra、J. C. Cresswell、G. W. Taylor和H. R. Tizhoosh，《用于组织病理图像分析的差分隐私联邦学习》，《科学报告》，第12卷，第1期，第12508页，2022年。[85] O. Choudhury、A. Gkoulalas-Divanis、T. Salonidis、I. Sylla、Y. Park、G. Hsu和A. Das，《面向敏感健康数据的差分隐私联邦学习》，NeurIPS ML4 02578，2019 1910 H Workshop；arXiv: 。[86] M. Blatt、A. Gusev、Y. Polyakov和S. Goldwasser，“使用同态加密开展安全的大规模全基因组关联研究”，《美国国家科学院院刊》，第117卷，第21期，第11 608–11 613页，2020年。[87] R. Geva、A. Gusev、Y. Polyakov、L. Liram、O. Rosolio、A. Alexandru、N. Genise、M. Blatt、Z. Duchin、B. Waissengrin等，“使用多方同态加密对肿瘤学数据进行协作式隐私保护分析”，《美国国家科学院院刊》，第120卷，第33期，文章编号e2304415120，2023年。[88] F. Khan、S. A. Shah、S. Tahir、Y. Yasin Ghadi、S. I. Shah、A. Zahid、J. Ahmad和Q. Hussain Abbasi，“智能医疗中的隐私增强技术：研究挑战与机遇”，《ACM计算评论》，2025年。[89] T. Geppert、S. Deml、D. Sturzenegger和N. Ebert，“可信执行环境：应用与组织挑战”，《计算机科学前沿》，第4卷，文章编号930741，2022年。[90] A. Paju、M. O. Javed、J. Nurmi、J. Savim¨aki、B. McGillion和B. B. Brumley，“综述：用于开发可信应用的可信执行环境使用情况系统综述”，载于《第18届国际可用性、可靠性与安全会议论文集》，2023年，第1–15页。[91] R. M. Rogers、A. Roth、J. Ullman和S. Vadhan，“隐私里程表与过滤器：按需组合”，《神经信息处理系统进展》（NeurIPS），第29卷，2016年。[92] S. P. Kasiviswanathan、K. Nissim、S. Raskhodnikova和A. Smith，“使用节点差分隐私分析图”，载于《密码学理论会议》（TCC 2013）。施普林格，2013年，第457–476页。[93] M. Hay、C. Li、G. Miklau和D. Jensen，“对隐私网络度分布的准确估计”，载于《2009年IEEE国际数据挖掘会议》（ICDM），2009年，第169–178页。[94] M. Tian、B. Chen、A. Guo、S. Jiang和A. R. Zhang，“通过扩散模型可靠生成隐私保护合成电子健康记录时间序列”，《美国医学信息学会杂志》，第31卷，第11期，第2529–2539页，2024年。[95] S. Truex、N. Baracaldo、A. Anwar、T. Steinke、H. Ludwig、R. Zhang和Y. Zhou，“隐私保护联邦学习的混合方法”，载于《第12届ACM人工智能与安全研讨会论文集》（AISec），2019年，第1–11页。[96] K. Bonawitz、H. Eichner、W. Grieskamp、D. Huba、A. Ingerman、V. Ivanov、C. Kiddon、J. Konečnỳ、S. Mazzocchi、B. McMahan等，“迈向大规模联邦学习：系统设计”，《机器学习与系统会议论文集》（MLSys），第1卷，第374–388页，2019年。[97] B. McMahan、E. Moore、D. Ramage、S. Hampson和B. A. y Arcas，“基于去中心化数据的深度网络通信高效学习”，载于《人工智能与统计学》（AISTATS）。PMLR，2017年，第1273–1282页。[98] D. Froelicher、J. R. Troncoso-Pastoriza、J.-P. Bossuat、M. H¨ahnel、V. Belagiannis、P. Frossard、A. Geissb¨uhler和J.-P. Hubaux，“利用多方同态加密实现精准医学中真正的隐私保护联邦分析”，《自然·通讯》，第12卷，第1期，文章编号5910，2021年。[99] J. Ficek、W. Wang、H. Chen、G. Dagne和E. Daley，“健康研究中的差分隐私：范围综述”，《美国医学信息学会杂志》，第28卷，第10期，第2269–2276页，2021年。[100] N. Khalid、A. Qayyum、M. Bilal、A. Al-Fuqaha和J. Qadir，“医疗保健中的隐私保护人工智能：技术与应用”，《生物学与医学中的计算机》，第158卷，文章编号106848，2023年。[101] “标准化数据：OMOP通用数据模型（OHDSI）”，https: //www.ohdsi.org/data-standardization/，2020年。[102] “PCORnet：国家以患者为中心的临床研究网络”，https://pcornet.org/，2025年。[103] C. Owsley、D. S. Matthies、G. McGwin、J. C. Edberg、S. L. Baxter、L. M. Zangwill、J. P. Owen和C. S. Lee，“人工智能就绪与公平糖尿病洞察图谱（AI-READI）的横断面设计与研究方案”，《英国医学杂志开放版》，第15卷，第2期，文章编号e097449，2025年2月。[104] G. Hripcsak、P. B. Ryan、J. D. Duke、N. H. Shah、R. W. Park、V. Huser、M. A. Suchard、M. J. Schuemie、F. J. DeFalco、A. Perotte等，“利用OHDSI网络大规模描述治疗路径”，《美国国家科学院院刊》，第113卷，第27期，第7329–7336页，2016年。[105] R. L. Fleurence、L. H. Curtis、R. M. Califf、R. Platt、J. V. Selby和J. S. Brown，“启动PCORnet：国家以患者为中心的临床研究

网络”，《美国医学信息学会杂志》，第21卷，第4期，第578–582页，2014年。[106] N. Homer、S. Szelinger、M. Redman、D. Duggan、W. Tembe、J. Muehling、J. V. Pearson、D. A. Stephan、S. F. Nelson和D. W. Craig，“利用高密度SNP基因分型微阵列解析向高度复杂混合物中贡献微量脱氧核糖核酸的个体”，《公共科学图书馆·遗传学》，第4卷，第8期，文章编号e1000167，2008年。[107] M. Gymrek、A. L. McGuire、D. Golan、E. Halperin和Y. Erlich，“通过姓氏推断识别个人基因组”，《科学》，第339卷，第6117期，第321–324页，2013年。[108] R. Pulivarti、J. Wagner、J. Zook、R. Craft、B. Kreider、J. Miller、P. O’Neil、C. Sames、J. Snyder、B. Stea等，“基因组数据网络安全与隐私框架社区档案”，美国国家标准与技术研究院，技术报告，2024年。[109] E. Yilmaz、T. Ji、E. Ayday和P. Li，“依赖型局部差分隐私下的基因组数据共享”，载于《第12届ACM数据与应用安全和隐私会议论文集》（CODASPY）。ACM，2022年，第77–88页。[110] N. Almadhoun、E. Ayday和 ¨O. Ulusoy，“依赖元组下的差分隐私：基因组隐私案例”，《生物信息学》，第36卷，第6期，第1696–1703页，2020年。[111] G. Qiao、W. J. Su和L. Zhang，“一次性差分隐私顶层选择”，载于《第38届国际机器学习会议论文集》。PMLR，2021年，第8672–8681页。kD. Holtz、M. Zhao、S. G. Benzell、C. Y. Cao、M. A. Rahimian、J. Yang、J. Allen、A. Collis、A. Moehring、T. Sowrirajan等，“未协调应对新冠肺炎的相互依赖性与成本”，《美国国家科学院院刊》，第117卷，第33期，第19 837–19 843页，2020年。[112] A. Collis、K. Garimella、A. Moehring、M. A. Rahimian、S. Babalola、N. H. Gobat、D. Shattuck、J. Stolow、S. Aral和D. Eckles，“关于新冠肺炎相关信念、行为与规范的全球调查”，《自然·人类行为》，第6卷，第9期，第1310–1317页，2022年。[113] D. A. Henderson，“天花的根除——过去、现在与未来概述”，《疫苗》，第29卷，增刊4，第D7–D9页，2011年。[114] M. J. Reid、R. Bunnell、E. K. Dokubo和J. Nkengasong，“PEPFAR中的项目科学：实现可持续艾滋病毒应对的路径”，《国际艾滋病学会杂志》，第27卷，增刊2，文章编号e26244，2024年。[115] M. Cinelli、W. Quattrociocchi、A. Galeazzi、C. M. Valensise、E. Brugnoli、A. L. Schmidt、P. Zola、F. Zollo和A. Scala，“新冠肺炎社交媒体信息疫情”，《科学报告》，第10卷，文章编号16598，2020年。[116] S. Loomba、A. de Figueiredo、S. J. Piatek、K. de Graaf和H. J. Larson，“衡量新冠肺炎疫苗错误信息对英国和美国接种意愿的影响”，《自然·人类行为》，第5卷，第337–348页，2021年。[117] I. Skafle、A. Nordahl-Hansen、D. S. Quintana和E. Gabarron，“社交媒体上关于新冠肺炎疫苗的错误信息：快速综述”，《医学互联网研究杂志》，第24卷，文章编号37367，2022年。[118] A. Nahum、D. M. Drekonja和J. D. Alpern，“公众信任的侵蚀与SARS-CoV-2疫苗——需要采取更多行动”，《开放论坛传染病学》，第8卷，第2期，文章编号ofaa657，2021年。[119] R. M. Carpiano、T. Callaghan、M. M. Mello、Y. A. Maldonado、R. DiResta、N. T. Brewer、C. Clinton、A. P. Galvani、S. B. Omer、J. L. Schwartz、J. M. Sharfstein和P. J. Hotez，“在新冠肺炎时期应对美国反疫苗行动主义的演变与扩张”，《柳叶刀》，第401卷，第967–970页，2023年。[120] M. A. Rahimian和M. P. Colaresi，“民主韧性与社会技术冲击”，《计算与数学组织理论》，第31卷，第236–257页，2025年。[121] K. M. Weiss、S. M. Goodreau、M. Morris等，“美国男男性行为者的自我中心性性网络：ARTnet研究结果”，《流行病》，第30卷，文章编号100386，2020年。[122] J. L. Juusola、M. L. Brandeau、D. K. Owens和E. Bendavid，“美国男男性行为者艾滋病毒预防暴露前预防的成本效益”，《内科学年鉴》，第156卷，第8期，第541–550页，2012年。[123] J. Kessler、J. E. Myers、K. Nucifora、N. Mensah、C. Toohey、A. Khademi、B. R. Schackman和S. L. Braunstein，“评估纽约市优先实施抗逆转录病毒暴露前预防的影响”，《艾滋病》，第28卷，第18期，第2683–2691页，2014年。[124] R. Kuan，“医疗保健领域采用人工智能将缓慢且困难”，《哈佛商业评论》，第10卷，第1页，2019年。

[126] C. Wang、J. Zhang、N. Lassi 和 X. Zhang，《利用人工智能开展医疗保健中的隐私保护：中国法规的比较视角》，《Healthcare》，第10卷第10期，第1878页，2022年。[127] 《可识别个人身份的健康信息隐私标准（HIPAA 隐私规则）》，https://www.hhs.gov/hipaa/for-professionals/priv acy/index.html，2002年，美国卫生与公众服务部。[128] 《2008年遗传信息非歧视法（GINA），第110–233号公法》，https://www.eeoc.gov/statutes/genetic-information-nondiscrimination-act-2008，2008年。[129] 《联邦人类受试者保护政策（共同规则），《联邦法规》第45编第46部分（2018年要求）》，https://www.hhs.gov/ohrp/regulations-and-policy/regulations/45-cfr-46/index.html，2018年。[130] 《NIH数据管理与共享政策》，https://sharing.nih.gov/data-management-and-sharing-policy，2023年。[131] P. Kairouz、H. B. McMahan 等，《联邦学习的进展与开放问题》，《机器学习基础与趋势》，第14卷第1–2期，第1–210页，2021年。[132] F. Tramer、N. Carlini、W. Brendel 和 A. Madry，《关于针对对抗样本防御的自适应攻击》，《神经信息处理系统进展》，第33卷，第1633–1645页，2020年。[133] S. Neel、A. Roth 和 S. Sharifi-Malvajerdi，《下降删除：用于机器遗忘的基于梯度的方法》，载于《算法学习理论》（ALT）。PMLR，2021年，第931–962页。[134] A. Ginart、M. Guan、G. Valiant 和 J. Y. Zou，《让人工智能忘记你：机器学习中的数据删除》，载于《神经信息处理系统进展》（NeurIPS），第32卷，2019年，第3518–3531页。[135] K. Bonawitz、V. Ivanov、B. Kreuter、A. Marcedone、H. B. McMahan、S. Patel、D. Ramage、A. Segal 和 K. Seth，《隐私保护机器学习的实用安全聚合》，载于《2017年ACM SIGSAC计算机与通信安全会议》（CCS）论文集，2017年，第1175–1191页。[136] J. Abowd、R. Ashmead、S. Garfinkel、D. Kifer、P. Leclerc、A. Machanava- jjhala 和 W. Sexton，《Census TopDown：差分隐私数据、增量模式以及与公共知识的一致性》，美国人口普查局，技术报告，2019年。[137] 《实践中的隐私保护数据共享》（PDaSP），NSF 24-585，美国国家科学基金会，项目征集公告，2024年。