人工智能医疗器械创新合作平台
ARTIFICIAL INTELLIGENT MEDICAL DEVICE INNOVATION AND COOPERATION PLATFORM

数字疗法数据安全评价研究报告

人工智能医疗器械创新合作平台数字疗法工作组

2025 年

本文件为北京市科技计划项目《精神疾病数字疗法产品测试验证技术服务平台构建及应用》的研究成果，可作为产品设计开发和成品检验的技术参考，不具有强制性。

前 言

数字化浪潮正在重塑医疗健康的未来图景。作为数字医疗领域的重要组成部分，数字疗法作为一种由软件驱动、基于循证医学证据的疾病干预手段，正逐渐成为医疗健康领域的创新焦点。它通过数字化技术对患者进行疾病预防、管理和治疗干预，不仅拓展了传统医疗的边界，也为同时实现提高医疗质量、提升可及性和降低医疗成本这一目标提供了新的思路。随着数字疗法在全球范围内的快速发展，其价值与潜力日益凸显。数字疗法的核心特征在于其数据驱动的根本属性——它通过持续采集、分析和反馈患者的健康数据，直接对患者施加精准、可衡量的干预。这种干预模式高度依赖于从个人信息、诊断记录到实时生理参数等海量敏感健康医疗数据的处理与价值挖掘，使得数据安全成为其不可动摇的基石。

然而，伴随着数字疗法快速发展而来的是对数据安全问题的日益关切。数字疗法产品处理的大量敏感数据，其安全性直接关系到患者的生命健康和隐私权益。数据泄露、篡改、滥用等风险不仅可能对患者个人隐私造成无法挽回的损害，引发歧视与创伤，更可能因提供错误的治疗建议或中断治疗流程而直接导致医疗安全事故，危及患者生命。因此，构建以数据为核心的安全保障与评价体系，是数字疗法产

业得以健康发展的生命线。

本报告旨在系统探讨数字疗法的数据安全评价框架。报告将聚焦于健康医疗数据的全生命周期，从技术和管理两个维度深入分析在数据采集、传输、存储、使用、共享与销毁各环节面临的安全挑战与防护对策。我们将结合国内外数字疗法的发展现状和趋势，提出适合我国国情、并紧扣《数据安全法》《个人信息保护法》等法规要求的数据安全评价指标体系，为数字疗法产品的研发、应用和监管提供参考。

目 录

一、 数字疗法概述 1
（一） 数字疗法的内涵与发展脉络 1
（二） 数字疗法的关键技术与应用领域 2
（三） 数据安全：数字疗法发展的核心基石 4
二、 数字疗法数据安全技术评价 5
（一） 数据安全与隐私保护核心技术体系 5
（二） 支撑数据安全的网络与应用安全技术 7
三、 数字疗法数据安全管理与治理 9
（一） 数据安全治理体系与监管合规 9
（二） 数据全生命周期安全管理实践 10
（三） 数据安全审计、监督与应急响应 11
四、 数字疗法数据安全应用场景分析 11
（一） 基于数据流动模式的部署环境安全分析 11
（二） 基于数据敏感性与共享需求的疾病领域安全分析 13
（三） 特殊用户群体的数据安全与伦理考量 14
五、 数字疗法数据安全挑战与对策展望 15
（一） 数据安全治理与合规的核心挑战 15
（二） 数据安全技术实践与协同的瓶颈 16
（三） 构建可信数据生态的战略路径 17

图 目 录

图 1 应用场景安全需求矩阵图 14

表 目 录

表 1 数字疗法主要应用领域及示例 3

一、数字疗法概述

（一）数字疗法的内涵与发展脉络

数字疗法（Digital Therapeutics, DTx）是以软件程序驱动的、基于循证医学证据的医疗干预手段，能够直接向患者提供疾病治疗、管理和预防服务。这种直接干预模式使其具有高度的可复制性、知识经验的可积累性、相对较低的单次使用成本以及前所未有的触达便捷性。

数字疗法的本质是医疗服务在数字空间的深度映射与智能化重构。它通过持续、被动或主动的数据采集与先进的分析算法（如机器学习），实现了治疗方案的动态优化与个性化调整，从而形成了一个强大的“评估-干预-反馈-再评估”的闭环系统。例如，在焦虑障碍的干预中，整合了数字疗法的系统可通过可穿戴设备持续监测用户的心率变异性与睡眠质量，并引导用户定期完成情绪量表。算法基于这些多维数据，可动态调整个体化的认知行为训练强度，或在其生理指标暗示紧张加剧时，适时推送正念呼吸练习，从而实现对症状的更主动、自适应管理。这种自适应和预测性干预特性，相比传统静态治疗方案具体更好的治疗效果。

数字疗法的概念与实践最早起源于美国，其发展的关键里程碑是2017年美国FDA批准了全球首款处方数字疗法产品。在中国，产业虽起步较晚，但得益于“健康中国 2030”战略的引领，发展势头强劲。政策支持是关键驱动因素，例如海南省率先将数字疗法列入省级发展规划，旨在打造“数字疗法创新岛”。截至2024年，中国境内

获批的数字疗法产品数量已快速增长至 50 余款，应用领域广泛覆盖精神心理疾病、慢性病管理、神经系统疾病及康复治疗等，市场规模年均增长率持续超过 30%。

（二）数字疗法的关键技术与应用领域

数字疗法并非单一技术的产物，而是多学科、多技术融合创新的集大成者。其主要依托的关键技术集群包括：1）人工智能与机器学习：作为核心引擎，用于数据分析、模式识别、决策支持和治疗方案的个性化推荐。2）大数据分析技术：处理和分析海量、多源、异构的健康医疗数据，挖掘数据价值。3）扩展现实技术：包括虚拟现实(VR)、增强现实(AR)和混合现实(MR)，为用户创造沉浸式或增强式的治疗环境，尤其在心理疾病暴露疗法、疼痛管理和康复训练中效果显著。4）先进的人机交互技术：确保软件界面易于使用，体验友好，降低用户使用门槛。5）生物传感与神经反馈技术：实时采集生理信号，并反馈给用户，用于生物反馈治疗。

这些技术的深度融合，为数字疗法提供了强大的技术基础，使其能够通过数据驱动的个性化干预方案，实现对疾病的精准管理与治疗。数字疗法的应用领域十分广泛，目前已从早期的试点探索逐步渗透到主流临床科室。

具体而言，其应用已深入心脑血管疾病二级预防、糖尿病等代谢系统疾病的管理、哮喘/慢阻肺等呼吸系统疾病的监控、肿瘤患者的居家康复支持、抑郁症/焦虑症等精神心理疾病的干预与治疗、以及

青光眼/弱视等眼科疾病的视觉功能训练等诸多方向。2024 年，数字疗法已被权威机构列为医工交叉领域的十大科技创新热点方向之一，预示着其未来将渗透到更多临床科室，并逐渐成为标准治疗路径中的重要组成部分。

表 1 数字疗法主要应用领域及示例

应用领域	具体疾病示例	代表产品特点
精神心理疾病	抑郁症、焦虑症、药物成瘾	认知行为疗法软件、虚拟现实暴露疗法
慢性病管理	糖尿病、高血压、慢阻肺	用药管理软件、个性化健康指导系统
神经系统疾病	阿尔茨海默病、儿童注意缺陷多动障碍	认知训练软件、脑功能康复系统
康复治疗	运动损伤康复、脑卒中康复	远程监控系统、个性化训练方案

展望未来，数字疗法的技术融合将更加深入和广泛。例如，区块链技术的引入，可以为核心治疗数据提供不可篡改、可追溯的安全保障，增强数据的可信度与隐私保护水平。5G/6G 通信技术的超低延迟和高可靠性，将使得需要实时反馈的复杂远程手术康复指导、高精度远程操控治疗成为可能。在应用领域方面，数字疗法正从常见病向罕见病管理拓展，通过远程患者登记和数据分析，为小众疾病群体提供可及的干预方案；在传染病领域，通过整合可穿戴设备数据的数字疗法平台，可实现区域性的疫情监测与早期预警。这些应用场景的扩展

，不仅极大地提升了医疗服务的可及性和覆盖率，也强力推动了临床医学、信息科学、工程学、行为心理学等学科的跨领域深度合作。但与此同时，应用场景的复杂化也对数据安全、系统集成、互操作性以及伦理监管提出了前所未有的更高要求。

（三）数据安全：数字疗法发展的核心基石

随着数字疗法从受控的院内环境向复杂的院外环境(如患者家庭)扩展，其面临的安全挑战性质发生了根本性变化。在诸多安全维度中，数据安全已跃升为制约其可持续发展最关键、最核心的议题。数字疗法的有效性高度依赖于从患者端持续采集的海量、多源、高敏感度的个人健康信息，包括诊断记录、实时生理参数、用药依从性、行为数据乃至基因信息。这些数据贯穿于数字疗法产品的全生命周期，其安全性直接决定了产品的可信度与临床价值。

数据安全之于数字疗法的重要性，首先体现在其与临床有效性和患者安全的深度绑定。数据在生命周期任一环节出现安全问题，如采集失真、传输中被篡改、存储时泄露或被滥用，其后果远不止于隐私侵犯。它可能直接导致算法模型做出错误的治疗决策，轻则影响疗效，重则引发严重的医疗安全事故，直接危及患者生命。

其次，数据安全是建立多方信任的基石。数字疗法的生态系统涉及患者、医护人员、医疗机构、监管机构和支付方等多方主体。唯有建立起坚实的数据安全保障，确保数据的保密性、完整性和可用性，才能赢得患者的使用信心、医生的处方意愿、监管的批准放行以及支付方的报销认可。缺乏可靠的数据安全措施，任何创新商业模式都难

以规模化落地。

最后，健全的数据安全体系是保障数字疗法在合规轨道上快速发展的重要前提。随着《网络安全法》、《数据安全法》、《个人信息保护法》以及医疗器械相关法规的深入实施，对健康医疗数据的安全保护提出了明确的法定要求。数字疗法产品应将数据安全与隐私保护的要求内嵌于设计、开发、运营的全过程，遵循“数据最小化”、“目的限定”等原则，否则将面临巨大的法律与合规风险。

二、数字疗法数据安全技术评价

（一）数据安全与隐私保护核心技术体系

数据安全是数字疗法技术体系的基石，其目标是确保健康医疗数据在全生命周期内的保密性、完整性和可用性。这需要一套层次化、纵深化的核心技术体系作为支撑，该体系紧密围绕数据生命周期的各个环节构建。

在数据采集的源头，安全始于对数据质量和真实性的保障。数字疗法通过多样化的软硬件传感器采集数据，确保这些初始数据未被篡改或注入是首要任务。通过基础的设备认证，采用可信执行环境（TEE）等技术为关键数据采集流程提供隔离的、受硬件保护的安全区域，能有效防止恶意软件在采集环节伪造或窃取生理数据。同时，在数据产生的第一时间即实施分类分级打标，为后续差异化保护策略奠定基础，这符合数据安全治理的基本原则。

数据传输过程中的安全，是连接患者终端与云端分析平台的关键纽带。除了使用 TLS 1.3 等最新加密协议实现通道安全外，可以考虑

采用端到端加密（E2EE）的应用措施。在 E2EE 模型下，数据在发送端加密，仅在接收端解密，即使云服务提供商也无法访问明文数据，这为敏感健康数据在公共网络上的传输提供了最高级别的保密性。此外，引入数据完整性校验机制，如哈希函数或数字签名，可确保数据在传输途中未被篡改，一旦接收方验证失败即可请求重传，保障了数据的完整性。

数据存储环节的安全防护建议区分静态数据和动态数据。对于静态数据，建议采用高强度对称加密算法（如 AES-256）进行加密，而密钥本身宜通过硬件安全模块（HSM）或云服务商提供的密钥管理服务（KMS）进行安全存储和管理，实现密钥与数据的分离管理，极大提升破解难度。对于云上存储，应充分利用服务商提供的加密存储选项，并明确数据存储的地理位置以满足合规要求。数据库安全同样至关重要，建议通过严格的访问控制、字段级加密和数据库活动监控（DAM）来防止内部越权访问和拖库攻击。

数据使用阶段的安全挑战最为复杂，因其涉及数据的解密和处理。为实现在使用中保护数据，隐私增强技术（PETs）展现出巨大潜力。差分隐私技术可在统计查询或数据挖掘时向结果中添加随机噪声，使得无法从输出结果中推断出任何个体的信息，从而在释放数据价值的同时保护个人隐私，非常适合用于数字疗法的临床研究数据分析。同态加密技术则允许在加密数据上直接进行计算，计算结果解密后与在明文上计算的结果一致，这为外包数据分析（如第三方算法模型对加密数据进行分析）提供了可能，而无需暴露原始数据。联邦学习作

为一种分布式机器学习范式，算法模型被发送到各数据源（如不同医院的本地服务器）进行训练，仅汇总模型参数的更新，而非集中原始数据，这从根本上避免了数据汇聚带来的隐私泄露风险。

在数据共享与销毁环节，技术手段需与管理流程紧密结合。数据共享应遵循最小必要原则，通过数据脱敏技术（如对标识符进行假名化处理）在共享非必要敏感信息时降低风险。对于数据销毁，尽量采用不可逆的技术手段，对于存储介质上的数据，使用符合 NIST 800-88 等标准的安全擦除算法多次覆写；对于云上数据，确保其被彻底删除且备份副本也同步清理。所有数据共享和销毁操作建议具备不可否认的审计日志。

（二）支撑数据安全的网络与应用安全技术

数据并非存在于真空之中，其安全高度依赖于其所处的网络与运行其上的应用程序的安全。因此，网络安全与应用安全技术是保障数据安全不可或缺的支撑环境。

网络是数据流动的血管，网络安全技术为数据提供通道层面的保护。数字疗法产品部署环境的多样性（院内专网、家庭 Wi-Fi、移动网络）要求网络防护策略应具备适应性。在院外环境中，建议使用虚拟专用网络（VPN）或利用 5G 网络切片技术为数字疗法业务创建端到端的逻辑隔离专用网络，可以有效防止数据在公共互联网上被窃听或劫持。部署下一代防火墙（NGFW）和入侵检测/防御系统（IDS/IPS），基于深度包检测技术实时分析网络流量，能够有效识别和阻断针对数字疗法平台的网络攻击，如试图利用漏洞窃取数据的恶意扫描或

拒绝服务攻击（DDoS），后者通过耗尽资源使数据服务不可用，直接破坏数据的可用性。

应用是数据处理的载体，应用安全技术直接关系到数据能否被安全地处理和使用。在软件开发层面，遵循安全开发生命周期（SDLC），在编码阶段通过静态应用程序安全测试（SAST）工具扫描源代码以早期发现安全漏洞，在上线前通过动态应用程序安全测试（DAST）模拟黑客攻击进行渗透测试，是防止 SQL 注入、跨站脚本（XSS）等常见漏洞导致数据泄露的关键。对于数字疗法广泛依赖的应用程序编程接口（API），建议实施严格的安全管控，包括使用 OAuth 2.0 等标准协议进行认证和授权，对 API 调用进行速率限制和 throttling 以防止滥用，并记录详尽的 API 访问日志用于审计和异常行为分析。这些措施共同确保只有经过授权的请求才能访问和操作数据。

身份与访问管理（IAM）是连接用户、应用与数据的桥梁，是防止数据未授权访问的核心。在数字疗法场景中，建议实施多因素认证（MFA），结合密码与手机验证码、生物识别（如指纹、面部识别）等多种要素，极大提升攻击者冒充合法用户的难度。在此基础上，贯彻最小权限原则，通过基于角色的访问控制（RBAC）或更灵活的基于属性的访问控制（ABAC）模型，精细管控医生、患者、研究员等不同角色对数据的访问范围（如能否查看、修改、导出），确保每个用户仅能访问其履行职责所必需的最小数据集。所有权限的分配和变更都应有清晰的审计追踪。

最后，人因工程与安全设计虽不直接属于传统的数据安全技术范

畴，但其通过优化用户与产品的交互，间接对数据安全产生深远影响。一个设计拙劣的用户界面可能导致患者输入错误数据或误解治疗指示，从而影响数据的准确性和后续治疗的安全性。因此，简洁直观的界面设计、明确的操作指引、针对特殊人群（如视障患者）的无障碍功能，都能减少人为操作失误，从源头上提升数据质量与使用安全，是数据安全体系中不可或缺的“软性”技术组成部分。

三、数字疗法数据安全管理与治理

（一）数据安全治理体系与监管合规

构建系统的数据安全治理体系是实施有效管理的顶层设计。该体系的核心在于明确组织内在数据安全方面的决策权限、责任分工与协调机制。首先，企业可考虑设立专门的数据保护官或数据安全委员会，负责制定全局性的数据安全策略，并监督其执行。这一策略建议与企业的业务目标和风险偏好相一致，并自上而下地贯彻到所有部门。

在合规层面，数字疗法产品需满足日益严格的法规监管要求。中国的《数据安全法》与《个人信息保护法》共同构成了数据合规的基石，特别是对健康医疗等敏感个人信息处理活动提出了“告知-同意”的严格要求。数字疗法企业建议建立常态化的合规流程，包括数据保护影响评估（DPIA），用于系统性识别和降低新产品或新功能的数据处理风险。此外，积极参与行业自律，推动建立基于《信息安全技术 个人信息安全规范》等国家标准的具体实践指南，对于填补当前数字疗法专项标准缺失的空白至关重要。监管合规不仅是法律义务，更是构建患者信任、赢得市场准入的关键。

（二）数据全生命周期安全管理实践

数据安全管理应贯穿于数据从采集到销毁的每一个环节，这正是对第二章所确立的“数据生命周期”主线的具体管理实践。在数据采集阶段，管理重点可放在落实“最小必要原则”和“目的限定原则”。这需要通过严格的设计评审和隐私设计（Privacy by Design）流程来保证，确保仅收集实现治疗目的所必需的最少数据，并在产品设计阶段就向用户清晰、明确地告知数据收集使用的范围与目的。

在数据传输与存储阶段，管理的核心是加密策略与密钥管理的制度化。企业建议制定明确的加密算法标准（如采用国密算法或AES-256）和密钥轮换策略。对于云上存储，建议明确数据驻留要求，并与云服务商签订数据处理协议（DPA），明确双方的数据安全责任。在数据使用阶段，最关键的管理的任务是实施精细化的访问控制。这需要建立基于角色（RBAC）或属性（ABAC）的访问控制模型，并严格执行“最小权限原则”，确保医护人员、研究人员等不同角色只能访问其职责范围内的数据。所有对敏感数据的访问、查询、导出操作都尽量有详细、不可篡改的日志记录，为审计提供依据。

数据共享与销毁阶段是管理最容易出现漏洞的环节。数据对外共享宜建立在有效的法律协议（如数据共享协议）基础上，并采用脱敏或匿名化等技术手段降低风险。数据销毁则需制定明确的数据留存政策，在达到保留期限或收到用户删除请求时，执行标准化的、可验证的数据彻底删除流程。所有这些管理实践都应被文档化，形成可执行、可检查、可追溯的标准操作程序。

（三）数据安全审计、监督与应急响应

持续性的监督与审计是确保数据安全管理体系有效运行的保障机制。建议定期开展数据安全审计，内容包括技术审计（如检查访问日志是否存在异常、验证加密配置是否正确）和管理审计（如检查数据分类分级政策是否得到执行、员工培训记录是否完整）。审计可借助自动化工具，但更关键的是通过模拟攻击、渗透测试等方式主动发现防御体系的脆弱点。

建立专门针对数据安全事件的应急响应预案至关重要。该预案应区别于一般的网络安全事件预案，需明确数据泄露、数据篡改、数据滥用等特定场景的定级标准、报告流程（包括在法定时限内向监管部门和受影响个人报告）和处置措施。预案的核心目标是快速遏制事件影响、消除安全隐患、恢复系统运行，并进行彻底的根因分析以防止复发。定期的应急演练是检验预案有效性和提升团队响应能力的关键。最终，通过审计和应急响应中发现的不足，驱动数据安全治理体系与管理制度持续优化，形成一个完整的“计划-实施-检查-改进”（PDCA）闭环，从而动态提升组织的整体数据安全水位。

四、数字疗法数据安全应用场景分析

（一）基于数据流动模式的部署环境安全分析

数字疗法数据安全的具体实践并非千篇一律，其技术措施与管理策略的强度与侧重点，需根据具体的应用场景进行动态调整。本章将依据第二章所建立的数据生命周期与分类分级原则，深入剖析不同场景下数据安全的独特需求。

部署环境直接决定了健康医疗数据的流动路径与边界，是评估数据安全风险的首要因素。院内外不同环境的数据流模型差异巨大，安全架构也需随之演变。

在院内部署环境中，数字疗法产品通常深度集成于医院信息系统（HIS、EMR）中。其数据安全的核心挑战在于复杂的接口交互与内部数据共享。数据从患者端采集后，需流向医生工作站、医院数据中心乃至科研平台，流动路径复杂，接触点众多。此时，安全设计可以以建立严格的内部访问控制边界为重点。除了网络层的 VLAN 隔离，更关键的是在应用层实现基于角色的精细化数据权限管理，确保不同科室的医护人员只能访问其诊疗活动所必需的患者数据片段。所有跨系统的数据调用都建议通过安全的 API 网关进行认证、授权和审计，并记录详尽的日志，以实现数据在院内流转的全程可追溯。

相比之下，院外部署环境（如患者家庭）的数据流动模型相对简单，主要表现为患者终端向云端平台的点对点传输。然而，其安全环境不可控，数据安全面临更大威胁。此时，安全核心转向强化端到端的保护。在数据传输上，建议采用端到端加密（E2EE），确保数据离开患者设备后即处于密文状态，直至被云端服务解密，有效防范公共网络上的窃听风险。在数据存储上，应优先采用云端安全存储方案，并由患者控制核心数据的访问密钥。同时，应用程序需具备检测运行环境安全性的能力，如识别是否连接不安全的 Wi-Fi，并提醒用户或自动切换至更安全的移动网络。

而对于混合部署场景（如社区健康服务中心），数据则在局部边

缘节点与中心云平台间分段流动。安全架构需兼具院内的管理复杂性和院外的端点安全性。可采用边缘计算技术，在社区节点本地完成数据的初步处理和加密，仅将脱敏后的聚合数据或模型参数上传至云端，从而最大限度减少敏感数据在广域网上的暴露面。这种架构对数据进行了分布式保护，是平衡效率与安全的重要方向。

（二）基于数据敏感性与共享需求的疾病领域安全分析

不同疾病领域处理的健康数据在敏感度、规模及共享需求上存在本质区别，直接决定了数据安全措施的优先级。

精神心理疾病领域产生的数据，如心理评估结果、情绪记录、虚拟现实暴露疗法的沉浸式内容等，具有极高的个人敏感性。一旦泄露，可能对患者造成严重的社会歧视和心理二次伤害。因此，该领域的数据安全策略建议以隐私保护为最高优先级。在技术层面，除了强加密，应优先考虑采用隐私增强技术，如联邦学习，使得模型训练无需集中敏感数据。在管理层面，访问权限控制应极为严格，并可能需要对数据进行更高级别的匿名化处理后方可用于科研分析。

慢性病管理领域（如糖尿病、高血压）的数据特点是长期、连续、海量，其核心安全目标是保障数据的长期完整性与可用性。因为治疗决策依赖于对长期趋势的分析，任何数据篡改或丢失都可能影响治疗方案的准确性。同时，此类数据常需在患者、家属、医生、保险公司等多方间共享，因此安全的数据共享机制成为关键。需要设计灵活的访问策略，支持基于属性的动态授权，并利用区块链等技术为关键数据（如服药记录）打上不可篡改的时间戳，确保数据的可信度。

重大疾病或罕见病领域的数据价值极高，但患者群体小，数据格外珍贵。其安全需求突出体现在为促进医学研究而进行的安全数据协作上。在严格保护个人隐私的前提下，如何通过安全多方计算、差分隐私等技术，在加密状态或添加噪声后实现多中心数据联合分析，释放数据的科研价值，是该领域数据安全的前沿课题。

如图 3 所示，不同应用场景的数据安全需求可根据数据敏感度和数据共享频率两个维度进行定位，从而帮助开发者快速识别主要风险并采取针对性措施。

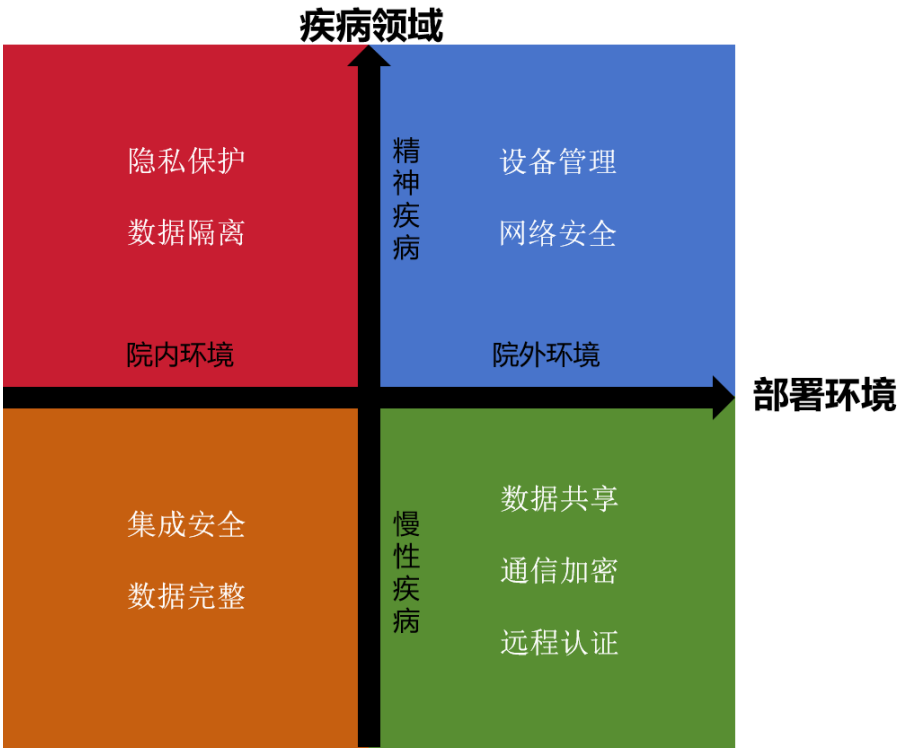

图 1 应用场景安全需求矩阵图

（三）特殊用户群体的数据安全与伦理考量

数字疗法需服务于包括老年人、儿童、认知障碍患者在内的多元用户群体，保障他们的数据安全需超越单纯的技术层面，融入更多的

人文与伦理关怀。

对于老年患者，其数据安全风险常源于非恶意的人员操作失误或对网络欺诈防范意识不足。安全设计需兼顾安全性与可及性，例如，在启用强密码认证的同时，提供生物识别或简化登录流程。更重要的是，应建立可靠的紧急联系人或多因素认证机制，在检测到异常活动（如异地登录）时，能通过子女或监护人的二次确认来阻止潜在的数据泄露风险。

对于儿童患者，数据安全的核心在于平衡监护与隐私。系统需为监护人提供必要的监督权限，以追踪治疗进展，但应严格限制其访问范围，防止过度监控侵害儿童隐私。同时，产品应向儿童提供与其认知水平相适应的、清晰易懂的数据使用说明，培养其早期的数据主权意识。

对于认知障碍患者（如阿尔茨海默病患者），其数据权利与决策能力可能随病情变化而减弱。这就迫切需要设计动态的数据代理决策机制。系统应允许患者在意识清醒时预先设定数据共享意愿和权限（如指定可信赖的家人），并在达到预设条件时自动启动代理决策模式，确保在其失去决策能力后，治疗数据仍能在保障安全的前提下用于其持续护理，这体现了数据安全设计中最深层次的伦理责任。

五、数字疗法数据安全挑战与对策展望

（一）数据安全治理与合规的核心挑战

数字疗法产业的蓬勃发展，使其所处理的健康医疗数据价值与风险同步攀升。通过前文分析可见，构建坚实的数据安全体系是产业可

持续发展的基石。然而，在实践道路上，我们仍面临一系列严峻挑战，亟需在技术、治理与生态层面寻求突破，方能在保障安全的前提下，充分释放数字疗法的巨大潜力。

在管理与治理层面，最突出的挑战源于数据权责的复杂性与合规路径的动态性。数字疗法涉及患者、医生、企业、医院、保险公司、监管机构等多方主体，数据在各方间流动，其所有权、控制权、处理权、受益权等权责边界往往模糊不清。例如，当基于患者数据训练的算法模型产生新的洞察时，其知识产权归属如何界定？这为建立清晰的数据安全责任体系带来了巨大困难。

同时，监管政策与标准仍处于快速演进期。虽然《数据安全法》《个人信息保护法》确立了基本原则，但针对数字疗法这一新兴领域的数据分类分级细则、匿名化标准、跨境传输规范等尚未明确，导致企业在合规实践中常常面临无据可依的困境。不同地区（如中国与欧美）的监管要求存在差异，也为产品全球化布局带来了复杂的合规成本。应对这一挑战，建议应由监管机构、行业组织与企业共同协作，加快制定细化的、场景化的数据安全标准与指南，并探索建立适应技术创新速度的敏捷监管模式，如基于风险的合规评估框架，为产业提供稳定且可预期的政策环境。

（二）数据安全技术实践与协同的瓶颈

在技术落地层面，挑战主要体现在安全、效率与成本之间的相互制约，以及技术协同的复杂性。以隐私增强技术为例，同态加密、安全多方计算等虽能提供极高的安全性，但其巨大的计算开销和通信延

迟在当前阶段难以满足数字疗法对实时性要求较高的交互场景(如实时生物反馈治疗)。联邦学习避免了原始数据集中，但对各参与方的数据质量和模型对齐能力提出了更高要求，且其自身仍存在隐私泄露的潜在风险。

此外，数字疗法产品通常整合多种硬件传感器、软件应用和云服务，构成一个复杂的技术栈。确保数据在这个复杂技术栈的每一个组件、每一次交互中都得到无缝的、端到端的安全保护，是极其困难的。任何一个薄弱环节的漏洞都可能成为整个数据防线的突破口。破解这一瓶颈，一方面有赖于计算硬件的持续革新和算法的不断优化，以降低隐私计算的技术门槛；另一方面，则需要推动建立标准化的安全接口与协议，促进不同安全技术模块之间的顺畅集成与协同工作，降低整体方案的复杂度和维护成本。

（三）构建可信数据生态的战略路径

面对上述挑战，数字疗法数据安全的未来发展建议超越单点技术的突破或单一企业的努力，着眼于构建一个共建、共治、共享的可信数据生态。这是一项系统工程，需要从以下战略路径着力推进。

一个可行路径是推动数据安全基础设施的现代化与普惠化。鼓励发展第三方安全即服务（Security-as-a-Service）平台，将复杂的加密服务、密钥管理、安全审计等功能模块化、云端化，使中小企业能以较低成本接入企业级的数据安全能力，降低整个行业的安全基线。

核心路径是探索建立基于规则与技术的可信数据流通机制。通过“监管沙盒”等创新模式，在保障安全的前提下，试点探索数据要素

市场化配置的新路径。利用区块链技术实现数据共享过程的不可篡改、可追溯；结合智能合约自动执行数据使用协议，确保数据使用符合预设规则。这能在保护隐私的前提下，促进数据在科研、保险精算等场景中的合规高效利用，释放数据价值。

长远路径在于培育深度融合的安全文化与人才体系。通过建立跨学科的教育和培训体系，提升患者群体的数据安全素养与权利意识，使其成为自身数据安全的积极参与者和监督者。唯有当安全成为内化于每个参与者心中的基本准则，可信数据生态才能拥有最稳固的根基。