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

数字疗法数据安全通用评估规范

人工智能医疗器械创新合作平台数字疗法工作组

2025 年 10 月

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

数字化浪潮正以前所未有之力重塑全球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（Digital Therapeutics, DTx）以其软件驱动、基于循证医学证据的核心特征，正迅速成为实现疾病预防、管理、治疗干预的创新焦点。它通过数字化技术拓展传统医疗边界，为同时实现提升医疗质量、可及性与降低医疗成本这一多重目标提供了全新的解决路径。随着数字疗法在认知障碍、精神心理疾病、慢性病管理等众多领域的应用日益深入，其临床价值与社会效益愈发凸显。

然而，数字疗法的快速发展与其对海量敏感健康医疗数据的深度依赖，也使其面临着严峻的数字安全挑战。数字疗法产品直接关乎患者生命健康与隐私权益，数据泄露、网络攻击或系统故障等安全事件不仅可能导致个人隐私严重受损，更可能直接引发错误的治疗决策，危及患者安全。因此，构建系统、科学、可操作的数据安全评估体系，是保障数字疗法产业健康、可持续发展的基石，也是推动其获得临床认可、通过监管审批、实现广泛覆盖的关键前提。

本规范旨在为构建一套适用于数字疗法产品数据安全评估框架提供参考，紧密结合数字疗法数据全生命周期的特点，从技术防护、管

理流程、应用场景等多个维度提出相应的测试方法。本规范的核心在于探讨数字疗法数据安全的关键考量维度，为产品研发机构、医疗机构、检测认证机构及监管部门提供测试参考。其内容涵盖数据安全与隐私保护技术、网络安全与通信保障、人因工程安全设计，以及贯穿产品全生命周期的安全管理要求，并针对不同部署环境、不同疾病领域及特殊人群的安全需求进行了差异化分析。

目 录

第一章 引言与概述 1
1.1 编制背景与目的 1
1.2 数字疗法定义与核心特征 1
1.3 评估规范框架简介 2
第二章 评估原则与整体框架 3
2.1 数据安全评估基本原则 3
2.2 数字疗法数据安全框架构成 4
2.3 评估指标体系概述 5
第三章 数据安全技术评估规范 6
3.1 数据安全与隐私保护技术评估 6
3.2 网络安全与通信安全评估 7
第四章 数据安全管理评估规范 8
4.1 监管政策与标准符合性评估 8
4.2 全生命周期安全管理评估 9
4.3 安全审计与应急响应评估 9
第五章 应用场景数据安全评估规范 100
5.1 不同部署环境下的安全考量评估 100
5.2 不同疾病领域的数字安全需求评估 111
5.3 特殊人群的数字安全考量评估 122
第六章 评估实施与持续发展 133

6.1 评估流程与实施方法 133
6.2 挑战与应对策略 133
6.3 持续改进与发展建议 144

第一章 引言与概述

1.1 编制背景与目的

随着全球数字化转型的深入发展，数字疗法（Digital Therapeutics, DTx）作为数字医疗领域的前沿方向，已展现出重塑疾病管理与健康服务模式的巨大潜力。其通过软件驱动的、基于循证医学证据的干预手段，为患者提供了可及性高、个性化强的疾病预防、管理与治疗新范式。然而，数字疗法产品的核心在于对患者健康数据的持续采集、分析与应用，这一特性使其面临着严峻的数据安全挑战。数据泄露、未授权访问、网络攻击等风险不仅直接威胁患者隐私权益，更可能因数据篡改或系统故障导致错误的治疗决策，危及患者生命安全。

当前，我国数字疗法产业在政策支持与技术创新的双轮驱动下进入快速发展期，但与之配套的数据安全评估标准体系尚不完善。现有规范多侧重于传统医疗器械或通用软件，难以完全契合数字疗法数据生命周期长、应用场景复杂、实时交互要求高的特点。这种标准缺失状态导致了市场产品安全水平参差不齐，为行业健康有序发展埋下了隐患。因此，本规范的编制旨在系统构建一套科学、统一、可操作的评估框架，为数字疗法产品的设计、研发、测试、应用提供相关参考。

1.2 数字疗法定义与核心特征

本规范所称的数字疗法（Digital Therapeutics, DTx），是指以软件程序为核心，基于循证医学证据，用于预防、管理或治疗医学定义下的疾病或病况的干预手段。其可直接向患者施加治疗性影响，亦可与其他药物、医疗器械或其他疗法协同使用。数字疗法并非简单的健康

管理软件，其核心特征在于:

1.干预的直接性与治疗性：数字疗法产品能够在医生指导下长期、不间断的对患者产生可测量、可评估的治疗效果。

2.数据驱动的闭环系统：数字疗法通过持续的数据采集（如来自传感器、用户交互）与先进算法（如机器学习），形成“评估－干预－反馈－再评估”的动态优化闭环，实现治疗方案的个性化调整，这是传统静态治疗方案无法比拟的。

3.高度的可复制性与可及性：基于软件的特性使其能够以较低成本大规模复制和分发，特别有助于提升医疗资源匮乏地区的服务可及性。

4.知识经验的可积累性：在治疗个体患者的同时，聚合的匿名化数据为医学研究提供了宝贵资源，能够反哺医学科学进步，形成从治疗个体到优化方案、普惠大众的正向循环。

正是这些核心特征，使得数字疗法的数据安全至关重要。其数据不仅关乎个人隐私，更直接关联治疗决策的有效性与安全性，因此有必要建立专门的安全评估体系予以保障。

1.3 评估规范框架简介

本规范的整体框架设计遵循系统性、层次性和可操作性的原则，旨在全面覆盖数字疗法数据安全的关键维度。规范主体共分为六章，逻辑结构如下:

第一章 引言与概述：阐明编制背景、目的、核心概念，为后续章节提供基础。

第二章 评估原则与整体框架：确立评估工作需遵循的基本原则，并勾勒出由技术、管理、运营构成的多维安全框架，为具体评估提供顶层指导。

第三章 数据安全技术评估规范：聚焦于数据生命周期的各个环节（采集、传输、存储、使用、共享、销毁），详细规定加密、访问控制、网络安全、隐私保护技术等方面的具体评估指标与方法。

第四章 数据安全管理评估规范：从组织、制度、流程层面出发，规定在政策合规、全生命周期安全管理、安全审计、应急响应及供应链安全等方面的管理要求和评估标准。

第五章 应用场景数据安全评估规范：针对数字疗法在不同部署环境（如院内、院外）、不同疾病领域（如精神心理、慢性病）以及面向特殊人群（如老年人、儿童）应用时的特定安全需求，提出差异化的评估要点。

第六章 评估实施与监督机制：明确评估的具体流程、方法、责任主体以及持续监督改进的机制，确保本规范能够有效落地执行。

各章节内容相互关联，共同构成一个从原则到实践、从通用到特殊的完整评估体系，旨在为数字疗法数据安全保驾护航。

第二章 评估原则与整体框架

2.1 数据安全评估基本原则

数字疗法数据安全评估工作的有效开展，应建立于一套科学、系统且具备指导性的核心原则之上。评估活动需首先秉持风险导向原则，将识别、分析和评价特定应用场景下的数据安全威胁与脆弱性作为起

点，并依据风险等级合理分配评估资源，确保将关注焦点集中于高风险领域。同时，建议坚持生命周期全覆盖原则，将评估视角贯穿于产品从需求分析、设计开发、测试验证、部署运营直至最终退市销毁的完整生命周期，确保每个阶段的安全控制措施均得到有效验证，避免出现安全盲区。

此外，评估工作宜严格遵循隐私保护与合规性原则，确保产品在全流程中符合《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律法规的强制性要求，并将隐私保护 Privacy-by-design 理念深度融入产品设计与运营。评估还需体现技术与管理并重原则，深刻认识到仅依靠技术防护或仅依赖管理规范均无法构建完整的安全防线，应综合考察技术手段与管理流程的协同配合能力，以形成有效的纵深防御体系。最后，评估过程自身应保证客观性与可重复性，即评估方法、流程和判断准则应明确、统一，使得不同评估主体在相同条件下对同一产品进行评估时，能够得出客观、一致的结论，从而维护评估结果的公信力。

2.2 数字疗法数据安全框架构成

为系统化地开展评估工作，本规范构建了一个由技术安全、运营安全和管理安全三个核心维度相互交织、协同作用的整体评估框架。该框架旨在形成一个多层次、纵深防御的有机体系。技术安全维度是框架的基础支撑，侧重于通过具体的技术手段实施基础防护，其评估范围广泛涵盖数据安全与隐私保护技术、网络安全与通信安全保障、严格的身份认证与精细的访问控制、安全的编码实践与系统配置基线

以及符合人因工程学的安全设计等方面，确保从技术底层构建稳固的防御能力。

运营安全维度则关注安全措施在产品持续运行过程中的动态有效性、适应性与韧性，重点评估是否建立并有效执行了持续的安全监控与日志分析机制、系统化的漏洞管理流程、完备的安全事件应急响应预案以及基于定期审计与演练的持续改进机制。管理安全维度作为框架的顶层设计与制度保障，重点评估组织是否建立了确保政策法规合规的内部制度，是否明确了安全组织架构与人员职责并开展了有效的安全意识教育，是否实施了定期的风险评估与管理工作，以及对第三方组件和服务供应商是否实施了有效的供应链安全管控。需要强调的是，技术、运营、管理这三个维度并非孤立存在，而是紧密关联、相互依赖的。先进的技术手段需要依靠严谨的管理制度和灵活的运营流程来保障其持久有效性，而顶层的管理要求则需要通过具体的技术方案和持续的运营活动来落地执行。因此，评估时建议综合考察三者的一体化融合与协同程度。

2.3 评估指标体系概述

为确保评估工作可量化、可操作，并能准确反映数字疗法数据安全的整体水平，本规范在上述框架下设计了一套结构清晰、分层级的评估指标体系。该体系由评估类、评估项和评估要点三个层级构成，旨在系统性地分解和落实数据安全要求。评估类对应于评估框架中的最高层次和关键领域，例如“数据生命周期安全”、“应用安全”、“网络安全”、“隐私保护”、“组织与制度安全”等，它们共同勾勒出评估

的范围全景。

在每个评估类之下，进一步细化为若干具体的评估项，例如在“数据生命周期安全”这一评估类下，可设立“数据采集安全”、“数据传输安全”、“数据存储安全”、“数据使用与共享安全”、“数据销毁安全”等多个评估项，从而将宏观要求分解到具体环节。评估要点则是评估项下的最小可验证单元，它明确规定了具体的评估内容、可采用的评估方法（如文档审查、工具测试、访谈、现场观察）以及清晰的符合性判定准则（如“完全符合”、“部分符合”、“不符合”）。此指标体系的设计充分考虑了数据在生命周期不同阶段所面临的各异风险与相应控制措施的变化，旨在通过系统化、标准化的指标设置，为衡量数字疗法产品的数据安全状况提供一个客观、全面且具可比性的评价标尺，指导后续具体的评估实践。

第三章 数据安全技术评估规范

3.1 数据安全与隐私保护技术评估

数据安全是数字疗法安全体系的基石，其评估需重点关注数据全生命周期的保护措施。在数据采集环节，评估应验证采集过程的合法合规性、数据源的可靠性以及数据质量的准确性，确保通过传感器、用户输入等多元化方式采集的数据真实有效。数据传输环节需评估端到端加密技术的应用强度，例如是否采用符合要求的 TLS 协议版本，并对证书管理机制进行严格审查，防止数据在传输过程中被窃听或篡改。数据存储环节的评估要点包括存储介质的物理与逻辑安全、加密算法的强度以及密钥管理的完备性，尤其是对静态数据采用高强度加

密并结合硬件安全模块的保护措施。

隐私保护技术的评估需与法律法规要求紧密结合。重点审查是否在产品设计阶段即融入隐私保护理念，是否遵循数据最小化原则仅收集必要信息，以及在临床研究等场景下是否恰当运用匿名化、假名化或差分隐私等技术平衡数据可用性与隐私保护。评估还需涵盖用户权利保障机制，如是否提供清晰的数据查询、更正、删除路径，是否建立严格的基于角色或属性的访问控制体系确保数据仅被授权人员访问。对于数据共享场景，建议评估其知情同意机制的完善性、数据使用目的的限制性以及第三方数据接收方的安全管理能力。

3.2 网络安全与通信安全评估

网络安全评估旨在检验数字疗法产品抵御外部攻击和保障业务连续性的能力。评估范围需覆盖其所有可能的部署环境，包括医疗机构内部网络、家庭 Wi-Fi、公共网络以及移动蜂窝网络等。对于院内部署，应重点评估其与医院信息系统的集成安全性，如网络边界隔离强度、访问控制策略的严密性以及对潜在内部威胁的防范能力。对于院外部署，评估则需关注在不可控网络环境下的安全防护，例如是否强制使用 VPN 或专用通信通道，是否具备检测和应对网络钓鱼、恶意软件入侵等威胁的能力。

通信安全评估侧重于保障数据在传输过程中的完整性与保密性。需详细审查所有通信链路所采用的安全协议及其配置是否达到业界最佳实践标准，例如是否禁用不安全的旧版协议并优先使用 TLS 1.3 等现代加密协议。同时，应对应用程序接口（API）的安全性进行深

入评估，包括身份认证、授权机制、输入验证及防滥用措施，防止通过 API 接口发起的攻击。对于依赖云平台的数字疗法，评估还需延伸至云服务提供商的安全资质及其与企业共同承担的安全责任划分，确保云环境的基础设施安全、平台安全及应用安全均得到有效管控。

第四章 数据安全管理评估规范

4.1 监管政策与标准符合性评估

管理层面的评估首先在于审视数字疗法产品全生命周期是否符合国家及行业相关的法律法规与标准规范。评估活动需系统核查产品在研发、注册、部署、运营各阶段是否满足《网络安全法》、《数据安全法》、《个人信息保护法》以及医疗器械相关监管法规（如《医疗器械软件注册技术审查指导原则》、《医疗器械网络安全注册技术审查指导原则》）的强制性要求。重点评估数据分类分级管理制度的建立与执行情况，个人信息处理活动的合法依据（如知情同意）的获取与维护情况，以及跨境数据传输（如适用）的合规性。

同时，评估需考察组织对国际标准（如 ISO 27001 信息安全管理体系、ISO 27799 健康信息安全管理）和行业标准（如 YY/T 0664 医疗器械软件生命周期过程）的采纳与内化程度。这不仅要求组织拥有相关的标准认证证书，更关键的是评估其是否将标准要求切实转化为内部的管理制度、操作流程和工作指令，并形成完整的符合性证据链条。评估还应关注组织对新兴法规和标准动态的跟踪与适应能力，确保其管理体系的持续合规性。

4.2 全生命周期安全管理评估

全生命周期安全管理评估要求对数字疗法产品从概念提出到最终退市的每一个阶段进行系统性的安全审查。在设计阶段，评估重点在于是否进行了充分的威胁建模和隐私影响评估，是否明确了安全目标与安全需求，并将这些要求准确传递至开发环节。在开发阶段，需评估安全开发生命周期的执行情况，包括安全编码规范的遵循度、静态与动态应用程序安全测试的集成、第三方组件的安全管理以及代码签名的应用等。

测试阶段的评估需验证安全功能的有效性，通常通过渗透测试、漏洞扫描、安全配置核查等方式进行，确保产品在上线前已知风险得到有效处置。在部署与运营阶段，评估转向持续性的安全管理，包括评估漏洞管理流程的及时性与有效性、安全配置的持续监控、变更管理的严格控制以及安全意识的常态化培训。产品退市阶段的评估则关注数据迁移或销毁方案的可行性与彻底性，确保患者数据得到妥善处理，防止遗留数据泄露风险。整个评估过程强调各阶段间的衔接与信息传递，确保安全管理的连续性。

4.3 安全审计与应急响应评估

安全审计机制评估旨在检验组织是否建立了独立、客观的监督检查体系以保障安全管理要求的落地。评估内容包括内部审计制度的完备性、审计计划的系统性、审计活动的执行频率与深度以及审计发现问题的整改跟踪与闭环情况。需审查审计记录是否完整、准确，是否覆盖技术系统（如日志审计、配置核查）与管理流程（如制度执行、

人员操作）两个方面，并能对数据处理活动提供足够的可追溯性。

应急响应评估则侧重于组织应对突发安全事件的能力。评估需核查是否制定了详实且可操作的应急响应预案，预案内容是否覆盖不同类型和等级的安全事件（如数据泄露、系统中断、网络攻击），是否明确了应急响应团队的组成、职责与联络机制。更重要的是，评估应通过审查演练记录、访谈关键人员等方式，检验预案的有效性及团队的实战能力，包括事件发现、分析、遏制、消除、恢复以及事后总结改进的全流程。评估还需考察是否建立了与监管机构、用户及公众的安全事件沟通预案，以符合法规要求并维护声誉。

第五章 应用场景数据安全评估规范

5.1 不同部署环境下的安全考量评估

数字疗法产品的部署环境多样性对其数据安全提出了差异化的评估要求。对于在医疗机构内部网络环境部署的产品，评估重点在于其与医院现有信息系统的安全集成能力。这包括评估其网络边界防护策略是否有效，能否实现与医院 HIS、PACS 等系统的安全数据交换，身份认证机制是否能够与医院单点登录系统无缝兼容，以及审计日志是否能够与医院安全事件管理平台有效对接。此类环境通常具备专业 IT 支持，但需严防因单点安全漏洞导致对整个医疗网络产生连锁风险。

对于在患者家庭、社区等院外环境部署的产品，评估面临更为复杂的挑战。这类环境网络可控性差，设备管理难度高，评估需重点关注终端设备自身的安全防护能力、在公共或家庭 Wi-Fi 等不可信网络

中的通信安全措施（如强制 VPN 或专用通道的使用），以及应对设备丢失、被盗等情况的远程数据擦除与锁定功能。混合部署环境（如社区医疗中心）则需兼顾院内院外双重特性，评估应考察其是否采用边缘计算等技术在本地处理敏感数据以减少云端传输风险，是否通过轻量级容器等技术实现应用隔离与安全管控，并评估其在不同网络环境间切换时的安全策略一致性及数据传输的连续性保障。

5.2 不同疾病领域的数字安全需求评估

不同疾病领域的数字疗法产品，因其处理数据的敏感性、干预方式的特殊性以及目标用户的差异性，在数据安全方面存在独特的评估侧重点。用于精神心理疾病干预的数字疗法，通常涉及极其敏感的情绪、心理评估及治疗对话记录，其数据泄露可能导致严重的个人声誉损害与社会歧视。对此类产品的评估，建议强调隐私保护的严格性，需重点评估其数据加密强度、匿名化处理深度、访问控制力度以及是否具备防止非授权访问的额外技术措施，确保患者内心最私密的信息得到最高级别的保护。

慢性病管理类数字疗法产品（如用于糖尿病、高血压管理）则需要长期、连续地收集患者的生理指标、用药记录、生活方式等数据。评估重点在于数据的连续性与完整性保障机制，防止数据缺失或篡改影响长期治疗决策的准确性。同时，此类产品常需与多家医疗机构、医生、保险公司等进行数据共享，评估需深入考察其数据共享接口的安全性、共享过程中的授权与审计机制，以及是否遵循最小必要原则进行数据交换。康复治疗类产品可能结合 VR/AR 等沉浸式技术，评

估需关注这些新技术引入的新型安全风险，如虚拟环境中的用户行为数据采集边界、设备传感器数据的安全处理等。此外，对于传染性疾病监测或罕见病管理等特定领域的产品，还需分别评估其数据实时处理能力与匿名化要求之间的平衡，以及针对小规模用户群体的经济可行的安全方案。

5.3 特殊人群的数字安全考量评估

数字疗法产品的广泛适用性要求其应充分考虑老年患者、儿童患者、认知障碍患者等特殊人群的使用特点与安全需求，评估工作需对此给予特别关注。针对老年用户群体，评估应侧重产品设计的易用性与安全引导的明确性。需检验用户界面是否简洁、字体大小是否合适、操作步骤是否足够简化，是否提供了清晰的语言或图示指导以避免误操作。同时，需评估产品是否包含针对老年人常见的网络诈骗、信息泄露风险的提醒与防护功能，帮助他们安全地使用数字疗法。

对于面向儿童患者的产品，评估需超越常规的数据安全范畴，延伸至内容安全与使用行为管理。需重点评估产品是否具备有效的家长或监护人监控机制，确保治疗过程在安全可控环境下进行；是否对使用时长、强度进行合理设置与提醒，防止沉迷；以及产品内的游戏化元素、多媒体内容是否存在诱导不当行为或潜在安全风险。对于认知障碍患者使用的产品，评估要点在于界面交互设计是否能有效降低使用过程中的困惑与焦虑感，例如是否采用高对比度色彩、明确的导航标识、简化的决策流程。同时，需评估其监护人机制的设计是否合理，能否在保障必要监护参与的同时，充分尊重并保护患者的隐私尊严，

实现数据访问权限的精细化管理与平衡。

第六章 评估实施与持续发展

6.1 评估流程与实施方法

为确保数字疗法数据安全评估的规范性与可操作性，建议建立清晰、标准的评估流程与多样化的实施方法。评估流程通常始于评估准备阶段，该阶段需明确评估目标、范围（如针对特定产品版本、特定功能模块或全系统）、依据的标准规范以及评估团队的组成与资质要求。紧接着是方案制定阶段，需基于产品特点和安全风险研判，确定具体的评估内容、评估指标（依据本规范前述章节）、评估方法组合（如文档审查、工具测试、访谈、现场观察）及时间计划。

评估执行阶段是核心环节，评估方需按照既定方案，系统性地收集证据，并依据评估要点进行符合性判定。在此过程中，可能综合运用多种方法：通过文档审查检验管理制度与设计文档的完备性；利用自动化安全扫描工具或手动渗透测试验证技术防护措施的有效性；通过对开发人员、运维人员、安全管理人员的访谈了解流程的实际执行情况；通过观察产品部署环境和操作过程确认配置与实操的一致性。评估结束阶段则侧重于结果分析与报告编制，需对发现的问题进行风险评级，分析根本原因，并提出针对性的整改建议，最终形成全面、客观的评估报告，作为产品改进和决策的基础。

6.2 挑战与应对策略

数字疗法数据安全评估在实践中面临着一系列技术与管理的挑战，识别这些挑战并制定相应的应对策略至关重要。技术层面，主要挑战

源于数字疗法技术的快速迭代与复杂性，例如人工智能算法的动态更新特性使得传统静态评估方法难以适用，多种硬件设备与软件平台导致的异构数据环境增加了数据质量与一致性评估的难度，以及新兴技术（如联邦学习、区块链）应用带来的新型安全风险评估经验不足。应对这些挑战，需要推动评估方法的革新，探索适应 AI 算法的动态评估与持续监控机制，加强基于标准化的数据接口与格式规范的一致性测试，并鼓励评估机构与产业界、学术界合作，前瞻性研究新技术应用的安全评估框架。

管理层面的挑战同样不容忽视，包括监管政策与标准仍处于发展完善期所带来的不确定性，行业内在安全能力与认知水平上的差异，以及具备医疗、技术和安全知识的复合型评估人才短缺。解决措施包括加强行业协同与引导，积极参与国际国内标准规范的制定与协调，推动建立行业最佳实践共享平台与威胁信息共享机制，大力发展针对性的专业人才培训与资格认证体系，从而逐步提升行业整体安全水平与评估一致性等。

6.3 持续改进与发展建议

数字疗法数据安全评估并非一次性活动，而是一个需要持续改进、动态发展的长期过程。首先，应建立评估结果的反哺机制。每一次评估活动中发现的问题、总结的经验，都应被系统性地分析，用于优化更新评估规范本身、改进评估方法工具，并为行业提供共性的风险警示和最佳实践指南。评估机构与企业应基于评估发现，制定并跟踪落实整改措施，实现闭环管理，并将安全改进纳入产品的版本迭代计划

中。

面向未来，为促进数字疗法数据安全评估体系的健康发展，建议从多方面着力。一是鼓励技术创新与融合，支持隐私计算、轻量级密码技术、安全多方计算等在评估中的应用研发，提升评估的效率和深度。二是完善检测认证生态体系，推动国家级、行业级数字疗法安全检测平台建设，鼓励第三方检测认证机构发展，并建立评估结果的互认机制，降低企业合规成本。三是强化国际合作与交流，积极参与国际标准规则的制定，推动中国方案与国际接轨，通过跨国研究与合作提升评估的前瞻性和全球视野。最终，通过构建一个技术先进、标准统一、执行有力、持续演进的数据安全评估体系，为数字疗法产业的健康、可信、可持续发展提供坚实保障。