君合专题研究报告

JUNHE

2022 年 7 月 27 日

人工智能在医疗健康领域应用涉及的数据合规问题

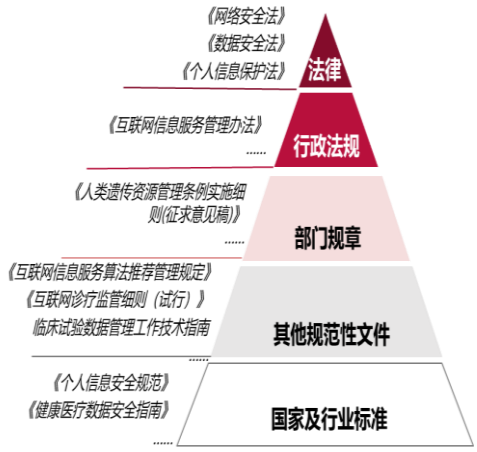
人工智能简单来说，就是研究如何使计算机去做只有人才能做的智能工作，通常用来描述不同类型的技术，包括机器学习、深度学习、神经网络等。随着人工智能的发展，近几年来，人工智能技术已经广泛地应用在辅助诊疗、药物研发、医学影像、健康管理等医疗健康领域。有关人工智能在医疗健康领域应用场景的详细介绍，请参考君合法评丨人工智能与医疗健康产业系列研究之一：人工智能在医疗健康领域的应用场景及监管政策概览。

人工智能的核心是通过计算机模拟或实现人类的学习行为，经大量的学习和实践以获得新的知识或技能，重新组织已有的知识结构使之不断改善自身的性能。在计算机学习的过程中，需要使用海量的数据，并基于一定的算法形成相应的知识体系。数据和算法是计算机学习的基础和底层逻辑，数据源的可靠、合法以及算法逻辑的科学、公平等都是形成计算机智力的重要因素。同时，无论在研发阶段还是应用阶段，医疗健康领域的人工智能技术往往涉及对患者、医生、受试者以及健康设备使用者的个人信息的采集与处理，且很可能涉及敏感个人信息和重要数据，因此个人信息及隐私保护以及重要数据的保护是人工智能在医疗健康领域应用的重要议题。本文将针对医疗健康领域的人工智能技术涉及的主要数据合规问题进行梳理和介绍。

一、 医疗健康领域人工智能的法律监管框架

医疗领域人工智能技术应用所涉及的数据合规相关的法律法规纷繁复杂。一方面，需要遵守网络安全、数据安全、个人信息保护相关的普遍适用的法律，以及与算法相关的法律法规；另一方面，也需要遵守医疗健康领域特殊的行业规定，包括医疗健康信息、遗传资源信息、病例资料管理、群体诊疗数据以及药品试验数据等相关的行业规定。此外，如果医疗健康智能产品依托于网站平台、App、小程序等互联网渠道提供服务，则还需要遵守该等平台相关的数据合规要求。

从效力层级区分：



从效力层级区分：

二、医疗健康领域人工智能技术涉及的主要数据合规问题

（一）算法合规

1、 算法透明性

当人工智能技术应用于诊疗、慢性疾病管理、健康管理等场景时，很可能涉及对患者、受试者健康信息的分析处理，通过算法模型分析的结果对与患者的诊断、健康管理及治疗计划可能产生重要的影响。举例而言，某款慢性疾病管理 App 可能会通过患者每日输入的信息（每日用药、心跳、血压、体重、睡眠状况等），分析和判断患者身体状况是否稳定。若经分析后判读认为患者存在疾病恶化的情况下，给出去医院就诊的建议；若经分析后认为患者病情稳定，则建议居家观察。App 的分析和判断尽管没有给出具体诊断建议，但其作出的是否去医院就诊的提示也会对患者造成重要影响。若 App 存在建议错误的情况，可能耽误患者的就医或者在患者病情并未恶化的情况下频繁要求其赴医院就诊。

对于此类应用算法技术进行分析与自动化决策，且决策结果可能对相关个人权益产生影响的情况，我国对相关数据处理者及算法服务提供者提出了披露义务。我国《个人信息保护法》（简称“**《个保法》**”）第 24 条规定，利用个人信息进行自动化决策的个人信息处理者应当保证决策的透明度，且通过自动化决策方式做出对个人权益有重大影响的决定，个人有权要求处理者予以说明。《互联网信息服务算法推荐管理规定》也规定了算法推荐服务提供者应当以显著方式告知用户其提供算法推荐服务的情况，并以适当方式公示算法推荐服务的基本原理、目的意图和主要运行机制等。通常，数据处理者或算法服务提供者可以通过用户手册、隐私政策、系统软件面板、语音等显著方式向相关使用者告知算法的基本原理、目的、运行机制、可能对个人产生的影响等。

除了算法透明性以外，如仅通过自动化决策的方式做出对个人权益有重大影响的决定，个人有权拒绝。如果该自动化决策功能植入在某款 App 中，则该 App 应提供个人拒绝的便捷渠道，通常建议在 App 中加入关闭该功能的选项。关于“对个人权益有重大影响”中如何认定“重大影响”，目前我国立法尚未明确进行解释。欧盟《通用数据保护条例》（简称“**GDPR**”）规定，对于仅依靠自动化处理作出的严重影响数据主体权益的决策，数据主体有权拒绝。对于 GDPR 下的“严重影响数据主体权益”的认定，欧盟的 WP29 工作组制定的关于《个人自动化决策与人物画像指南》（Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679）对严重影响数据主体权益的事项进行了列举，其中包括影响个人获得健康服务的决定。参考欧盟法相关解释，并考虑到健康普遍对于患者、受试者个人权益影响重大以及医疗健康领域本身的敏感性和重要性，通常涉及到对患者、受试者疾病、健康等做出分析和判断比较容易构成对相关个人的重大影响。

2、 算法偏见

数据样本偏差、算法逻辑瑕疵、算法设计者动机等因素均可能导致算法产生偏向性结果。例如，人工智能可能结合基因分析技术，测算出易患某种

特定疾病的人群，或基于既往保险理赔数据分析，定位出容易触发理赔的群体，进而对相关群体做出拒保或其他不合理收取高额保费的决策。又如，基于在医疗费用上的支出金额不同，向不同人群提供不同等级的健康护理产品。美国《科学》杂志发表的一项研究表明，美国医院中广泛使用的一种为患者分配医疗保健产品的算法已经系统地对白人和黑人进行了区分。该算法基于“健康需求越高，医疗保健费用通常也越高”这一基本逻辑，根据一年中累积支出的总医疗保健费用为患者进行了风险评分，并根据风险评分为患者分配不同的护理产品。研究后发现与白人相比，该算法向黑人提供针对“有复杂医疗需求的患者”所设计的护理项目的可能性很低。从数据来看，平均每年向黑人提供的护理费比向具有相同数量慢性病的白人提供的护理费少 1800 美元。这也意味着，黑人只有在患更严重的疾病时才会得到特定的救助。由此可见，算法技术应用于医疗健康领域若产生偏见，极易对于个人权益产生重要影响。

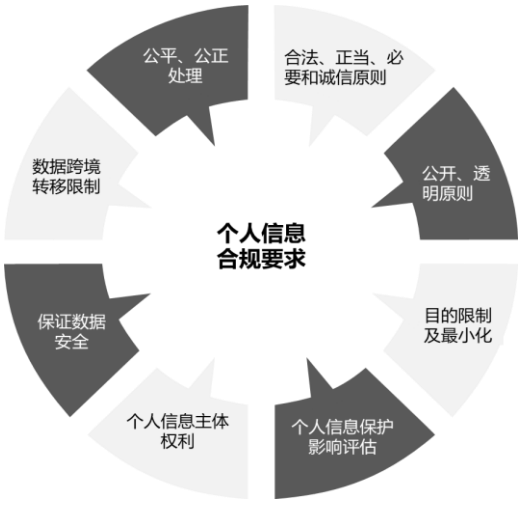
关于算法可能导致的偏见问题，我国《个保法》要求个人信息处理者利用个人信息进行自动化决策的，应保证决策结果的公平公正。《互联网算法推荐管理规定》也要求算法推荐服务提供者不得根据消费者的偏好、交易习惯等特征对其实施不合理的差别待遇。技术上，开展算法需要根据相关规定开展机器学习算法安全评估以及互联网信息推荐技术影响评估等工作。该等评估工作中也将算法是否可能存在偏见歧视纳入评估考虑。我国总体对于算法的偏见问题规定的较为原则性，尚未有专门的标准识别人工智能技术中的偏见。

对于算法偏见问题，美国国家标准与技术研究院 NIST 在 2022 年 3 月发布了《建立一个识别和管理人工智能中的偏见的标准》（Towards a Standard for Identifying and Managing Bias in Artificial Intelligence），旨在识别人工智能算法可能存在的偏见，并提出了框架性的处理建议。该标准将算法偏见分为系统偏见、人为偏见和数据/计算偏见三大类，并提出规避算法偏见的有效做法是对算法进行动态监测，并始终保持算法逻辑的可追溯性、可追责性，通过内部政策、程序规定、文件记录等方式降低算法偏见的危害。

（二）个人信息保护要求

1、 一般个人信息的合规要求

人工智能技术在医疗健康领域应用往往会涉及收集和处理患者、医生、受试者或健康管理软件使用者的个人信息，因此需要遵守有关个人信息处理的合规要求。总体而言，人工智能技术的个人信息合规要求归纳为以下方面。



合法、正当、必要和诚信原则的核心是任何个人信息处理行为必须具有合法依据。《个保法》提供了七项[1]处理个人信息的合法依据。其中，在医疗

[1] 《个人信息保护法》第十三条规定，符合下列情形之一的，个人信息处理者方可处理个人信息：（一）取得个人的同意；（二）为订立、履行个人作为一方当事人的合同所必需，或者按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需；（三）为履行法定职责或者法定义务所必需；（四）为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需；（五）为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息；（六）依照本法规定在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息；（七）法律、行政法规规定的其他情形。依照本法其他

健康领域的场景下，最常用的合法依据为取得相关个人同意，以及订立、履行合同所必须。在特定情况下，也可能依赖“紧急情况下为保护自然人的生命健康和财产安全所必需”，但该合法依据仅适用于危及自然人生命安全和财产安全的情况下，且由于情况紧急而无法获得相关个人同意的场景，因此适用极为有限。

公开、透明原则指的是个人信息处理者必须以显著方式、清晰易懂的语言真实、准确、完整地向相关个人告知其有关个人信息处理的相关事项。包括（1）个人信息处理者的名称或者姓名和联系方式；（2）处理目的、处理方式，处理的个人信息种类、保存期限；（3）行使个人权利的方式和程序；（4）若涉及处理敏感个人信息，则说明处理敏感个人信息的必要性以及对个人权益的影响；（5）若涉及算法、自动化决策，应说明算法的基本原理、目的意图和主要运行机制等。除此之外，如果涉及向其他个人信息处理者提供个人信息或者向中国境外提供个人信息，还有额外的披露要求。

个人信息保护影响评估的要求是当特定情况发生时，个人信息处理者必须开展个人信息保护影响评估。其中，触发个人信息保护影响评估的事项包括涉及处理敏感个人信息、自动化决策等。医疗健康场景下极有可能涉及处理敏感个人信息且人工智能技术也很可能涉及自动化决策，因此触发个人信息保护影响评估的可能性较大。

个人信息主体权利是个人信息主体在《个保法》下享有的一系列权利，包括个人信息的访问权、删除权、修改权、要求停止或限制处理权、可携带权、投诉权等，并且个人信息处理者应提供便捷的方式对个人信息主体权利进行处理。通常如果通过互联网、App、小程序等载体向个人提供医疗健康服务，建议在智能产品上提供便捷地行使该等权利的功能按钮。

过度收集个人信息一直以来是执法重灾区，在研发医疗健康人工智能产品时，应特别注意收集个人信息的范围，遵守**目的限制及最小化原则**，在设计人工智能产品时，将此原则纳入产品涉及的考虑，仅收集必要的信息。

2、 医疗健康相关的敏感个人信息

医疗健康领域涉及的数据往往包含个人健康信息、生物识别信息等，此类个人信息属于敏感个人信息，由于其一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害，因此会受到更为严格的监管要求。 此外，人工智能技术若应用于基因测序、细胞免疫疗法，还可能涉及人类遗传信息，而人类遗传信息的监管相比敏感个人信息更为严格。

《个保法》第 28 条明确将“生物识别”、“医疗健康”信息均属于敏感个人信息。除此之外，对于医疗健康信息的具体范畴，《信息安全技术 个人信息安全规范》给出了更细致的列举。根据该规范，个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等信息，均属于敏感个人信息；对于生物识别信息，该规范也进行了列举，包含个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等。

在目前常见的医疗健康人工智能产品中，诸多涉及上述敏感个人信息。例如人工智能技术辅助诊疗决策、互联网医院、慢性疾病健康监测、智能护理产品、智能穿戴设备、健康管理 App 等应用场景中，均可能涉及上述敏感个人信息，从而需要遵守敏感个人信息处理的额外合规要求。值得注意的是，不满十四周岁未成年人的所有个人信息都属于

有关规定，处理个人信息应当取得个人同意，但是有前款第二项至第七项规定情形的，不需取得个人同意。

敏感个人信息，处理其信息应获得其父母或监护人的同意。

3、 敏感个人信息处理的特殊要求

特定目的及充分必要性、告知义务： 如上文所述，处理敏感个人信息相比于处理一般个人信息更为严格，有更高的合规义务。其中，处理敏感个人信息必须具有特定目的和充分的必要性，并且在处理敏感个人信息之前，必须向相关个人告知处理敏感个人信息的必要性以及对个人权益的影响。

单独同意：处理敏感个人信息应当取得个人信息主体的单独同意。关于单独同意的获取，如果人工智能产品是通过 App、小程序或其他载体进行，则应当在收集敏感个人信息之前，通过弹窗、告知以及用户点击同意的方式获取相关的单独同意，并建议在产品中加入该等特定功能的开关按钮，实现用户便捷撤回同意的请求。此外，处理不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的同意。

严格保护措施：处理敏感个人信息需要采取严格的保护措施。关于保护措施的要求《信息安全技术 个人信息安全规范》规定，传输和存储个人信息需要采用符合管理要求的密码进行加密、个人生物识别信息应与个人身份信息分开存储、对于生物识别信息原则上仅存储摘要信息。

个人信息保护影响评估：如上文所述，处理敏感个人信息是触发开展个人信息保护影响评估的事项之一。在收集和处理敏感个人信息之前，应当进行个人信息保护影响评估工作。评估事项包括个人信息的处理目的、处理方式等是否合法、正当、必要，对个人权益的影响及安全风险，所采取的保护措施是否合法、有效并与风险程度相适应。个人信息保护影响评估报告和处理情况记录应当至少保存三年。

人类遗传信息：如果涉及处理基因组等人类遗传资源信息，则采集、保藏、买卖、利用和对外提供该等信息需遵守《人类遗传资源管理条例》、《人类遗传资源管理条例实施细则》等相关法规的额外规定，履行相关的审批、备案要求。

（三）重要数据的保护要求

除个人信息外，医疗健康领域的人工智能技术的应用还可能涉及重要数据，从而需要遵守重要数据的额外要求。对于重要数据的范围，根据信息安全标准化技术委员会 2022 年 1 月发布的最新版《重要数据识别指南》，反映群体健康生理状况、族群特征、遗传信息等的基础数据，如人口普查资料、人类遗传资源信息、基因测序原始数据属于重要数据。

参考上述指南的列举，医疗健康领域的人工智能应用的诸多场景可能涉及重要数据。例如，人工智能研发应用场景中，算法的筛选与决策可能基于对大量药品试验数据、医疗器械试验数据的分析；智能防疫监测场景中，智能回访功能的机器人可能会对病原进行追踪并收集相关数据；基因测序、精准防治的场景中可能涉及对于批量人类遗传信息的分析与测算；人工智能辅助诊疗的场景中，人工智能作出的诊断建议的可能基于对批量健康医疗数据各类诊疗与健康管理数据的分析处理。

重要数据的处理除了符合一般的数据保护要求外，还需符合额外的规定。包括，重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任；重要数据处理者应当对数据处理活动定期开展风险评估，并将风险评估报送至有关主管部门。重要数据出境还应当向相关网信部门申报数据出境安全评估。

（四）医疗类 App 的数据合规

医疗健康类人工智能产品的许多功能依托于

App、小程序或网页渠道实现的。例如，健康手环作为一种常见的可穿戴设备，通常与对应的手机App绑定使用。手环安装的智能传感设备采集到用户的心率、运动状态、睡眠情况等相关健康信息后，自动同步至App，用户可以通过App访问自己的健康数据，或上传其他相关信息，以生成更准确的健康报告、接收更适合个人的智能监测建议等。又如，慢性病护理系统，依托小程序将提供语音识别等交互体验方式，为心衰患者提供基本身体指征录入、日常问题问答、用药提醒、权威心衰知识等服务，协助心衰患者及家人对心衰疾病进行管理。除了健康监测之外，智能医院也可借助App实现便捷管理。例如，医生通过App随时录入查房、门诊、手术等相关文书，并同步导入院内系统。

在此前的App专项整治活动中，有许多医疗类App因侵害用户权益而受到通报，包括线上体检平台、糖尿病信息管理工具、孕妇诊疗平台、医美平台、线上医生工作台、智能诊疗系统、健康数据记录平台等。主要的违规行为包括违规收集和使用个人信息，超范围收集个人信息，强制、频繁、过度索取权限，强制用户使用定向推送功能，账号注销难，私自共享第三方等。

医疗类App除了应当符合有关个人信息、重要数据等合规要求。还应当遵守有关App的合规要求，具体合规要求可以参照《App违法违规收集使用个人信息自评估指南》、《常见类型移动互联网应用程序必要个人信息范围规定》、《移动互联网应用程序个人信息保护管理暂行规定（征求意见稿）》、《移动互联网应用程序信息服务管理规定》、《信息安全技术 移动互联网应用程序（App）收集个人信息基本要求》、《移动互联网应用程序（App）收集使用个人信息最小必要评估规范》等相关规定逐项审查。

（五）产品信息收集与医疗行业监管的博弈

在设计人工智能产品的同时，还需要兼顾医疗健康领域的其他监管要求，以避免收集特定信息或对信息的特定处理行为会触发医疗行业的特殊监管义务。

在开发医疗健康类人工智能产品时，应注意产品的功能、设计，评估是否落入医疗器械软件的范畴。若落入医疗器械的范畴，则应当根据医疗器械相关规定进行注册或备案。2022年3月9日，国家药监局器审中心网站发布《人工智能医疗器械注册审查指导原则》，进一步规范人工智能医疗器械的管理。

在开发医疗健康类人工智能产品时还可能需要考虑药品不良反应上报义务。 药品生产企业、药品经营企业、医疗机构在发现药品可能存在不良反应的情况下，必须向主管机关报告。倘若某疾病管理App产品收集患者服药情况，收集特定类型的信息可能会触发药品不良反应上报义务，这可能会额外增加对该疾病管理App上收集的信息的监管和筛查义务。但不收集该等特定信息又可能影响该智能产品的功能实现或用户体验。相关企业应当评估智能产品的目的，结合其相应的监管义务，决定收集信息的类型和范围以及智能产品的相关功能。

三、结语

随着我国人工智能技术的高速发展以及国家政策层面对于人工智能医疗健康产业的大力支持，人工智能技术在医疗健康领域的应用也将更广泛落地、相关产业市场规模的加速增长成必然趋势。人工智能产品在医疗健康领域的应用涉及的法律法规数量多、类型复杂。近年来，中国陆续出台《数据安全法》、《个人信息保护法》以及众多配套的法律、法规。各个行业也在陆续出台针对本行业的数据保护相关法规。随着人工智能技术的发展及广泛应用，有关算法和人工智能相关的法律、法规也预计会进一步出台，相关法律体系将逐渐完善。

无论是人工智能技术、算法技术还是医疗健康领域，其涉及的个人信息、数据等都较为敏感，合规要求严格。企业应当高度关注人工智能技术在医疗健康领域应用可能涉及的数据合规问题。

陆斯珮　合伙人　电话：86-10 2208 6250　邮箱地址：lusp@junhe.com
李沁璇　律　师　电话：86-21 2208 6187　邮箱地址：liqx@junhe.com