LINKS Law Offices
通力律师事务所

上海
上海市银城中路 68 号
时代金融中心 16/19 楼
电话: +86 21 3135 8666
传真: +86 21 3135 8600

北京
北京市建国门北大街 8 号
华润大厦 4 楼
电话: +86 10 8519 2266
传真: +86 10 8519 2929

香港
香港中环皇后大道中 5 号
衡怡大厦 27 楼
电话: +852 2592 1978
传真: +852 2868 0883

伦敦
1/F, 3 More London
Riverside, London SE1 2RE
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

通力法律评述 | 生命健康产业
2020 年 4 月

医疗健康 App 合规要点(下)——个人信息收集使用合规

作者：潘永建 | 邓梓珊

系列文章前言

互联网正以日新月异的速度改变着人们的生活。除了电商、外卖等，互联网医疗也越来越成为人们生活的一部分。当出现疾病症状时，人们往往习惯于在 APP 中进行在线诊断；需要前往医院时会在 APP 上进行在线挂号；需要购买药品也往往可以通过在线 APP 购得。除此之外，互联网医疗也已深入生活的更细微之处：我们的手表可以测量心率、心电图甚至血压，越来越多以前需要在医院才能完成的检测和评估现在可以自行在家完成。

飞速发展的互联网医疗技术也对企业合规提出了新的挑战和新的问题。药品在线销售的范围是什么?处方药是否可以在线销售?使用 APP 进行在线问诊、挂号、出售药械需要办理哪些电信资质?具备医疗监控、检测功能的 APP 或设备是否属于医疗器械?药品的运输与配送有何具体要求?互联网医疗中如何保护用户个人信息?这些都是互联网医疗无法避免的问题，但似乎又并非人人知道答案。

有鉴于此，通力律师结合法律与行业实践，针对互联网医疗专门起草了系列文章，以期能够更好地帮助互联网医疗从业者更好地理解法律法规与监管实践。**本文为系列文章第三篇：医疗健康 APP 合规要点(下)个人信息收集使用合规。**

随着大数据、云计算、物联网、人工智能等技术的飞速发展，互联网医疗市场规模不断扩大，“互联网+医疗健康”已然成为公共医疗机构、医药企业的业务拓展重点。前瞻产业研究院数据显示，预计 2020 年我国互联网医疗市场规模有望达到 900 亿元。移动医疗作为互联网医疗的一个重要分类，在改善就医体验、重配医疗资源、健康管理方面发挥着重要作用。

移动医疗是指借由移动互联技术以及各类移动互联平台提供的医疗保健服务。移动医疗服务的实现形式是多元化的。各类医疗健康类 App 是移动医疗最直观的表现形式，所能实现的功能基本已覆盖了诊前、诊中、诊后全程，包括：网络问诊、诊前咨询、网上挂号、网上支付、网上查询检验检查结果、健康教育与管理、医患交流、诊后随访、数据采集、慢病管理、远程监控、互联网药品销售、医生或病患社群等。医疗健康 App 的功能、需求和经营模式日益多样化，App 收集数据的渠道、种类以及收集处理的目的和方式随之变得更为繁杂。结合法规与从业经验，笔者将通过本文解析医疗健康 App 的合规要点，其中上篇基于医疗健康 App 的属性分析，剖析医疗健康 App 广告合规要点，下篇中分析医疗健康 App 相关个人信息收集使用的合规要点。

下篇

一. 医疗健康数据的属性

医疗健康数据的来源多样，包括病历信息、遗传病史、健康状况、医疗保险信息、实时身体机能指数、饮食结构、运动偏好等等。厘清该等数据的法律属性是合规收集、使用和处理的前提，我们梳理总结常见医疗健康数据的法律定义如下。

1. 个人信息/个人敏感信息——《网络安全法》

按照《网络安全法》和《信息安全技术 个人信息安全规范》(“《个人信息安全规范》”)，能够识别自然人个人身份而未进行匿名化处理的医疗健康数据都应属于法律意义上的“个人信息”。因此，App 用户输入的挂号身份信息、就诊记录、各项生理特征信息等都属于可以识别个人身份的信息。根据《个人信息安全规范》第 3.2 条以及附录 B 的列举，个人财产信息(如用户的交易和消费记录、银行账号等)、个人健康生理信息、个人生物识别信息(如 App 收集面部信息以实现在线咨询)、个人身份信息、网络身份标识信息(如账号、密码、口令等)等构成“个人敏感信息”，受更高程度的法律保护。

2. 人口健康信息——《人口健康信息管理办法(试行)》

人口健康信息是指各级各类医疗卫生计生服务机构在服务和管理过程中产生的人口基本信息、医疗卫生服务信息等人口健康信息，其中，电子信息与纸质文本具有同等法律效力。需要注意的是，虽然负责管理人口健康信息的责任单位为各级各类医疗卫生计生服务机构，但责任机构可以委托其他机构管理人口健康信息，委托单位也承担相应管理和安全责任。据此，提供在线挂号服务的 App 有可能收集、管理人口健康信息，需要承担相应责任。

3. 人类遗传资源——《人类遗传资源管理条例》

人类遗传资源信息是指利用人类遗传资源材料(含有人体基因组、基因等遗传物质的器官、组织、细胞等遗传材料)产生的数据等信息资料。未进行匿名化处理的人类遗传资源信息可能构成个人信息。对于人类遗传资源信息的收集、保藏、利用、对外提供均应遵守《人类遗传资源管理条例》相关行政审批程序的规定，并符合伦理原则，尊重人类遗传资源提供者的隐私。

4. 健康医疗大数据——《国家健康医疗大数据标准、安全和服务管理办法(试行)》("《管理办法》")

健康医疗大数据，是指在人们疾病防治、健康管理等过程中产生的与健康医疗相关的数据。根据该定义，几乎所有的医疗健康 App 所收集处理的数据均可构成健康医疗大数据。各级各类医疗卫生机构和相关企事业单位是健康医疗大数据安全和应用管理的责任单位。责任单位应当按照《管理办法》的规定履行健康医疗大数据管理职责。

5. 医疗器械相关数据——《医疗器械网络安全注册技术审查指导原则》("《指导原则》")

医疗器械相关数据从内容上可以分为健康数据和设备数据。健康数据指标明生理、心理健康状况的私人数据，涉及患者隐私信息。设备数据指的是描述设备运行状况的数据，用于监视、控制设备运行或用于设备的维护保养，本身不涉及患者隐私信息。对于构成医疗器械的医疗健康 App，运营者应当按照《指导原则》的要求，保证医疗器械网络安全，保持医疗器械相关数据的保密性、完整性和可得性。

6. 重要数据——《信息安全技术 数据出境安全评估指南(征求意见稿)》

重要数据是指一旦泄露可能直接影响国家安全、经济安全、社会稳定、公共健康和安全的数据，如未公开的政府信息，大面积人口、基因健康、地理、矿产资源，能够反映中国某地区的人口健康情况、疫情等。App 收集的医疗健康信息如果属于影响公共健康和安全的数据，则可能构成重要数据。

此外，《信息安全技术 数据出境安全评估指南(征求意见稿)》附录 A《重要数据识别指南》对人口健康类重要数据进行详细列举，包括但不限于：(1)在药品和避孕药具不良反应报告和监测过程中获取的个人隐私、患者和报告者信息；(2)突发公共卫生事件与传染病疫情监测过程中获取的传染病病人及其家属、密切接触者的个人隐私和相关疾病、流行病学信息等；(3)医疗机构和健康管理服务机构保管的个人电子病历、健康档案等各类诊疗、健康数据信息；(4)人体器官移植医疗服务中人体器官捐献者、接受者和人体器官移植手术申请人的个人信息；(5)人类辅助生殖技术服务中精子、卵子捐献者和使用者以及人类辅助生殖技术服务申请人的个人信息；(6)计划生育服务过程中涉及的个人隐私；(7)个人和家族的遗传信息等。

二. App 用户信息与隐私保护

对于 App 违规收集使用个人信息的行为，监管机关在加大处罚力度的同时越来越注重事前监管。2019 年 1 月 25 日，中央网信办、工业和信息化部、公安部及市场监督总局联合发布了《关于开展 App 违法违规收集使用个人信息专项治理的公告》，强调了网安法等法律法规提出的收集、使用个人信息的原则性要求，以及各政府主管部门在查处个人信息违法违规行为的职责，并提出由全国信息安全标准化技术委员会、中国消费者协会、中国互联网协会、中国网络空间安全协会(以上简称"App 专项治理工作组")制定 App 信息规范及违法违规收集个人信息治理评估要点。目前，App 专项治理工作组制定了**《App 违法违规收集使用个人信息自评估指南》**("《自评估指南》")，从隐私政策文本、App 收集使用个人信息行为、App 运营者对用户权利的保障等三大方面对 App 运营者做出了指引。其后，App 专项治理工作组最新公布了**《App 违法违规收集使用个人信息行为认定方法》**("《认定方法》")，列举了各类常见的 App 个人信息违规行为。此外，全国信标委于今年 1 月 20 日最新公布了**《信息安全技术 移动互联网应用(App)收集个人信息基本规范(征求意见稿)》**("《App 基本规范》")，对 App 收集个人信息列明管理方面及技术方面的要求，并以附录的形式列举了 21 种常用服务类型 App 可收集的最少信息、最小权限范围。

综上，按照《个人信息安全规范》等相关法规与规范性文件的要求，医疗健康 App 应从以下几个方面完善用户信息及隐私保护:

1. 完善隐私政策。考虑到用户可能包括了有生理缺陷的患者、老年人等弱势群体，隐私政策应尽量简洁、用户友好,并可使用图表帮助说明；用户安装、注册、第一次使用 App 前应采取增强式告知，提示关于个人信息收集的核心内容；以用户为中心，提供"一站式"撤回和关闭授权，在线访问、更正、删除用户个人信息，在线注销账户等功能；主动区分核心功能和附加功能提供用户选择，并告知核心业务功能所必须收集的个人敏感信息。

2. 获取用户知情同意；对于可能收集个人敏感信息的，应确保已取得用户的明示同意。不应通过捆绑 App 多项业务功能的方式，要求用户一次性接受并授权同意多项业务功能收集个人信息的请求。另外，应避免默示同意，根据用户主动填写、点击、勾选等自主行为，作为产品或服务的业务功能开启或开始收集个人信息的条件。对于个人敏感信息的收集，建议允许用户逐项选择是否提供或同意自动采集个人敏感信息。收集受试者个人信息的，应遵循受试者知情同意以及临床研究数据收集使用的有关规定。

3. 避免过度收集信息。遵循《个人信息安全规范》第 5.2 条提出的"最小化要求"，即收集的个人信息的类型应与实现产品或服务的业务功能有直接关联、自动采集个人信息的频率应是实现产品或服务的业务功能所必需的最低频率、间接获取个人信息的数量应是实现产品或服务的业务功能所必需的最少数量。

   另外，注意《App 基本规范》列明的各细分行业为实现服务所需收集的最少信息。例如:

类型	个人信息	使用要求/相关法律法规依据
问诊挂号 App	网络访问日志	仅用于满足《网络安全法》等相关法律法规要求和网络安全保障需要。通常包括 IP 地址、用户登录时间、用户退出时间等，并非指用户操作行为日志。
	手机号码	《移动互联网应用程序信息服务管理规定》
	交易信息	《电子商务法》 《网络交易管理办法》
	账号信息：账号、口令	仅用于标识问诊挂号用户和保障账号信息安全。
	患者身份信息	仅用于在预约挂号时对用户身份进行认证。
	医患沟通信息：性别、年龄、病情描述、过往病史、是否首诊	仅用于在线问诊时供当前医生判断患者病情。
	预约挂号信息：医科室	仅用于帮助患者完成预约挂号流程。
	第三方支付信息	仅用于用户使用第三方支付方式对问诊挂号订单付款，通常包括支付时间、支付金额、支付渠道等。

4. 告知如何使用自动数据收集工具。如果在 App 使用过程中，或是在 App 后台运行中有利用自动数据收集工具采集用户网络活动信息的情况，App 经营者首先应做到适度收集该类网络活动信息，不应超出与用户所约定的范围和目的收集信息；另外，App 经营者应在隐私政策中对使用的技术机制做详细描述，说明使用自动工具收集个人信息的目的，并向用户提供限制自动工具进行数据收集的方法和详细的指导。

5. 严格审核并管理与 App 提供服务相关的第三方，如数据处理服务方、云服务提供商等；定期检查审核 SDK、API 等接入方收集存储相关数据的情况，确保用户信息安全。

6. 如是通过医疗卫生机构共享而获取的医疗数据，则需设置患者数据保护防火墙，通过有效的脱敏措施，使收集到的数据无法识别特定个人且不能复原。

7. 注意域外法律可能的适用，尤其是域外法律针对医疗信息、疾病史等隐私信息和个人敏感信息的规定。

三. 医疗健康数据的本地化存储与跨境传输问题

1. 医疗健康数据若属于人口健康信息，各级各类医疗卫生计生服务机构不得在境外的服务器中存储，不得托管、租赁在境外的服务器。利用人口健康信息或为人口健康信息提供技术维护、支持的企业和个人(如相关 App 的技术提供方)虽然不属于《人口健康信息管理办法》的责任主体，但也需要遵守相关规定，做好企业合规工作，不应将服务器设在境外，或将相关数据传输至境外。

2. 医疗健康数据若属于人类遗传资源信息，外国组织、个人及其设立或者实际控制的机构不得保藏。若需要对外提供人类遗传资源信息的，应按规定进行申报或备案。

3. 医疗健康数据若构成重要数据，关键信息基础设施运营者需要将在中国境内运营过程中产生的个人信息和重要数据存储在境内，因业务需要确需传输的，需要进行数据出境安全评估。鉴此，App 运营者需要首先判定自身是否属于关键信息基础设施运营者，一旦构成关键信息基础设施运营者的，应当将个人信息和重要数据存储在境内。

4. 除对境内传输机构本身的要求外，国家标准《健康信息学 推动个人健康信息跨国流动的数据保护指南》还对数据导入方进行规制。数据控制方将医疗数据传输至另一国时，还需保证数据导入方采取组织和技术方面的安全措施充分保护传输数据，例如保密性、完整性等。

简言之，若 App 运营者无法确定对外(如向境外母公司、关联机构或第三方数据处理服务商)输出数据是否对国家安全、国计民生和公共利益构成危害，宜进行事前评估而避免盲目向境外传输具有一定敏感度的医疗健康数据。

四. 医疗健康 App 数据安全问题

医疗健康数据，尤其是患者的数据，蕴含着重要的科研价值和经济价值。与高价值特征相对应的是，健康医疗行业总体的网络安全风险级别通常处于“较大风险”。移动互联网安全在整体网络安全中的重要性尤为突出。中国信息通信研究院发布的《2019 健康医疗行业移动 App 安全观测报告》显示，健康医疗行业 App 安全风险集中体现在四个方面：一是安全漏洞风险居高；二是恶意程序危害严重；三是第三方 SDK 引入风险；四是安全加固比例偏低。具体而言，移动 App 网络安全相关的法律法规和标准体系不完善，极易给不法分子带来可乘之机；部分 App 开发流程不规范、更新修复不及时等问题较为突出；App 用户缺乏移动互联网安全意识，不良 App 使用习惯也会带来安全隐患。

解决 App 数据安全隐患、降低法律风险的首要任务是落实《网络安全法》规定的网络安全等级保护义务。其实早在 2011 年，卫生部就曾印发《卫生行业信息安全等级保护工作的指导意见》，要求在卫生行业全面开展信息安全等级保护定级备案、建设整改和等级测评等工作。在《国家网络安全检查操作指南》的关键信息基础设施业务判定表中，“医疗行业”中的“医院等卫生机构运营、疾病控制、急救中心运行”认定为关键业务；而在 2017 年公布的《关键信息基础设施安全保护条例(征求意见稿)》中，也将卫生医疗领域的单位纳入关键信息基础设施保护范围。考虑到《网络安全法》正式将落实网络安全等级保护制度作为法定义务，且对“关键信息基础设施”实行重点保护，广义上医疗行业的从业单位，即包括医疗健康 App 的运营者，均应严格落实等级保护制度，保证相关数据安全。

App 运营者应参照《信息安全技术 网络安全等级保护基本要求》，逐项落实网络安全保护措施：

1. 完成定级、测评、备案工作，落实网络安全等级保护制度。企业应注意到，定级备案和测评是分两步走的工作，完成定级和备案并不意味着等保工作的结束。

2. 制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任。
3. 采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施。
4. 采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月。
5. 采取数据分类、重要数据备份和加密等措施。

另外，App 使用 SDK、API 接口等第三方代码、插件协助进行数据的收集、传输和处理已经成为一种高效率的惯常做法，但第三方代码或插件收集数据时，通常不会主动告知、用户难以察觉，甚至有的 App 运营者本身也不清楚第三方代码或插件收集了哪些信息。而根据《信息安全技术 移动互联网应用程序(App)收集个人信息基本规范(征求意见稿)》，App 应对其使用的第三方代码、插件的个人信息收集行为负责。第三方代码、插件收集个人信息视同 App 收集，App 应防止第三方代码、插件收集无关的个人信息；但如果第三方代码、插件自行向用户明示其收集、使用个人信息目的、方式、范围，并征得用户同意，则第三方代码、插件独立对其个人信息收集行为承担责任。因此，App 运营者应审慎使用 API 接口等第三方代码、插件，宜采用合同等形式明确双方的安全责任及应实施的个人信息安全措施，并向个人信息主体明确告知。

如您希望就相关问题进一步交流，请联系：

潘永建
+86 21 3135 8701
david.pan@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系：**master@llinkslaw.com**

上海	北京	香港	伦敦
T: +86 21 3135 8666 F: +86 21 3135 8600	T: +86 10 8519 2266 F: +86 10 8519 2929	T: +852 2592 1978 F: +852 2868 0883	T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323

www.llinkslaw.com

Wechat: LlinksLaw

本土化资源 国际化视野