

《个人信息保护法》对生命健康行业的影响

作者：杨迅 | 象玉婷

《个人信息保护法》(以下简称“《个保法》”)已经于 2021 年 11 月 1 日正式生效,《个保法》是我国第一部在个人信息保护领域的综合性立法,将对各行各业产生重要的影响,尤其是生命健康行业。

1. 《个人信息保护法》概要

(一) 《个保法》及个人信息保护相关制度介绍

2018 年 9 月《个保法》首次被列入了我国的立法规划,后经三次审议并向社会广泛征求意见,在 2021 年的 8 月 20 日经第十三届全国人大常委会第三十次会议表决通过,并于 2021 年 11 月 1 日正式生效。

《个保法》作为个人信息保护领域的基础性法律,统一了个人信息的保护规则,无论是以电子形式还是纸质形式存在的个人信息,无论是员工信息、消费者信息或是其他个人信息,都将受到《个保法》的保护。《个保法》对个人信息的保护力度明显提升,对违法者的惩罚力度也显著加大。

《个保法》是关于个人信息保护的一个里程碑式的立法,但它并不是唯一的相关立法,其他一些法律和法规也有关于个人信息保护的规定。例如《民法典》中明确了自然人的个人信息受到法律保护;《刑法》中将非法获取和出售个人信息的行为定为犯罪;工业和信息化部于 2013 年发布的《电信和互联网用户个人信息保护规则》对通过提供电信服务和互联网信息服务过程中收集、使用用户个人信息的活动行为进行了规范。此外,生命健康行业的各监管机构也在各自的权限范围内发布了保护个人信息的相关规定,例如国家卫生健康委

For more Llinks publications,
please contact:

Publication@llinkslaw.com

如您需要了解我们的出版物,
请联系:

Publication@llinkslaw.com

员会(NHC)于 2014 年发布了《人口与健康信息管理办法》，其中包含了关于保护病历和健康信息的规定；国家药品监督管理局(NMPA)在 2020 年修订了《药物临床试验质量管理规范》，其中包括对受试者个人信息的保护。鉴于此，生命健康行业的企业在开展涉及个人信息的相关业务活动时，需要遵守包括上述法律和法规在内的所有相关规定。

(二) 执法动态展望

由于多部法律和法规都有关于个人信息保护的相关规定，因此各部门都将根据相关规定，在自身的权限范围内进行执法。根据《个保法》的规定，国家网信部门将负责统筹协调个人信息保护工作和相关监督管理工作；工信部将对通过应用程序和互联网门户收集和处理个人信息的相关活动进行监督执法；国务院有关主管部门在各自职责范围内负责个人信息保护和监督管理工作，例如国家卫生健康委员会将在医疗服务领域对涉及个人信息保护的相关活动开展执法检查，国家药品监督管理局将对药品临床试验、药品注册和不良反应报告等涉及个人信息保护的相关活动开展执法检查。

《个保法》加大了对侵犯个人信息行为的处罚力度，其中包括处以最高 5000 万元人民币的罚款或违法者上一年度营业额的 5%，并可以没收违法所得，责令停业整顿，或吊销经营许可证、营业执照等。此外，主管人员或其他直接责任人也可能被追究责任，并处以最高 100 万元人民币的罚款。被追究责任的个人在一定时期内将被限制担任董事、监事、高级管理人员或个人信息保护人员，构成犯罪的，将被依法追究刑事责任。值得注意的是，在个人信息相关的民事案件中，当个人信息处理者违反规定给个人造成损害时，“过错”的举证责任将被转移，由个人信息处理者承担，若其不能证明自己没有过错，根据《个保法》第六十九条的规定，则应当承担损害赔偿等侵权责任。

除此之外，《个保法》还规定了个人信息处理者侵犯个人信息的违法行为将会被记入信用档案并予以公示，对生命健康行业的相关企业而言，这样势必会对其声誉及公众形象造成严重的负面影响，不利于其业务的开展和持续经营。

《个保法》对生命健康行业将产生特别深刻的影响，作为处理个人信息最为密集的行业之一，制药公司、医疗器械公司和医疗服务提供者不仅收集和储存大量的病人和医疗服务专业人员的个人信息，往往还会涉及到与健康医疗相关的敏感个人信息，甚至是人类遗传资源和人口健康信息，这些信息对公众利益和国家安全至关重要，可以预见，生命健康相关行业将会成为个人信息保护的重点执法领域。

此外，随着近年来互联网业务的蓬勃发展，新兴的互联网技术在生命健康行业的应用越来越广泛，从而推动了数字化医疗业务的飞速发展，包括在线问诊服务、在线处方、远程医疗设备、数字化治疗等。应用程序、远程设备和其他终端被广泛用于收集、存储、处理和传输大量的个人信息，因此相关新兴企业需要密切关注《个保法》的合规要求以更好的履行个人信息保护义务。

2. 《个保法》对生命健康行业的挑战

《个保法》对生命健康行业的企业在个人信息的收集、处理、储存和转移等各方面都提出了严格的要求。

(一) 个人信息收集

生命健康行业对个人信息收集的场景包括：为个人提供诊疗、健康咨询；药品研发临床实验；医疗事故、药品及医疗器械的不良反应报告；健康险、寿险理赔等。线上及线下的相关企业在提供产品和服务的同时，不可避免的会涉及到诸如个人基本属性、健康状况信息、医疗应用信息、医疗支付等相关的个人信息及敏感个人信息。

根据《个保法》的规定，收集个人信息应当具有明确、合理的目的，且限于实现目的的最小范围，不得过度收集个人信息；其次，基于个人同意处理个人信息的，该同意应当是个人对处理目的、方式、种类充分知情的前提下自愿、明确作出的。再次，处理敏感个人信息(其中包括与健康有关的信息)需要有足够的必要性和个人的单独的同意。此外，若需要收集 14 岁以下未成年人的个人信息，则应当获得该未成年人父母或其他监护人的同意。

这些要求，虽然看起来简单明了，但在实践过程中却往往会给生命健康行业的相关机构和企业带来了不少的挑战。比如，对需要收集患者个人信息的制药公司而言，出于合规要求其可能无法直接接触到患者，这就给制药公司征求患者的同意造成了实际困难；再如，当制药公司直接向患者收集信息时(例如通过应用程序或其他互联网门户网站)，患者的个人信息可能是由其亲属提供的，这些个人信息是否来源合法，对制药公司来说常常难以确定。除此之外，在医学研究领域，研究机构(包括制药公司的研发部门)可能会在没有具体实验目的(即只有粗略的研究方向)的情况下从受试者那里收集大量的个人信息，由此就产生了相应的问题：这种情况是否违反了《个保法》中收集个人信息必须具有“明确目的”的要求？

(二) 个人信息的储存

根据《个保法》的规定，数据处理者必须(1)采取适当的管理措施及技术措施来保护其储存的个人信息；(2)不得将其收集的个人信息保留超过其处理目的所需的最短期限；(3)必须对其拥有的个人信息进行分类，并采用适当的保护措施。

上述规定要求企业在收集和储存个人信息时，采取必要的措施以保障个人信息的安全并满足合规的要求。然而在实践中，对生命科学领域的企业来说却存在不少问题。比如，当一家制药公司收到关于病人的信息时，这些信息可能会被用于不良反应报告、患者关爱服务、内部管理等多个方面，不同的部门需要收集处理不同类别的个人信息来实现各自的目标和功能。这就要求公司建立一个内部控制体系，只授予相关部门在其处理目的和功能实现基础上获取相应个人信息的权限；再如，在药品研发过程中收集的一些与健康有关的数据或与已获准销售的药品使用情

况有关的数据,可能会在没有具体目标的情况下长期储存,期望它们对未来的研究有所帮助。那么这种做法是否违反了关于个人信息储存“最短期限”的要求对相关企业来说值得商榷。除此之外,一些与医疗数据有关的个人信息储存受到相关法律法规的限制,例如按照法律的规定,患者的个人医疗记录应当被存储在医院的信息管理系统中,但这种限制就导致了其他医疗服务提供者与医院在共享医疗记录时的困难。

(三) 个人信息的转移

根据《个保法》的规定,个人信息的转移分为四种场景:(1)共同处理个人信息;(2) 对外提供个人信息;(3)委托处理个人信息;(4)在业务转移情况下的个人信息转移。《个保法》对不同场景下的个人信息转移提出了不同的要求,比如需要通知个人或取得个人的单独同意等,以确保个人信息的转移不会对个人信息的安全性造成不良影响。

生命健康行业的相关企业可能会在不同的场景中涉及到个人信息的转移,然而不同情况下的个人信息转移应当被归为上述哪一类别在实践中存在模糊地带。例如制药公司往往通过经销商来销售药品,并让经销商来收集病人的数据(特别是当经销商向患者直接交付药品时)。那么在这种情况下,制药公司和经销商之间的关系属于“对外提供个人信息”或“委托处理个人信息”的情形之一,这取决于由哪一方来确定患者个人信息收集的范围并对个人信息的收集处理活动负责。再比如当一家制药公司通过医院进行临床试验时,制药公司与医院之间并不一定是“委托关系”,因为医院也有自己的立场来收集受试者的个人信息。

(四) 个人信息出境

大多数生命健康行业的跨国企业需要面对数据出境的问题,因为它们需要在全球范围内处理在中国境内收集或产生的个人信息。根据《个保法》的规定,个人信息的出境必须满足以下条件之一:(1) 通过网信部门的安全评估;(2) 经专业机构认证;(3) 按照网信部门制定的标准合同与境外接收方订立合同。此外,在个人信息出境之前,相关个人信息处理者还必须按照规定进行个人信息保护影响评估。尽管《个保法》已经生效,但目前尚未对上述安全评估程序或认证程序进行规定,网信部门也没有发布个人信息出口的标准合同。那么,对相关企业而言,如何才能不影响个人信息继续出境,并降低合规风险呢?

生命健康行业的企业在许多场景下涉及个人信息的出境的问题,比如对于在全球范围内获得批准的药品,相关药品生产企业需要向多个国家的监管部门报告药品不良反应,由此不可避免的会产生了个人信息跨境传输的问题;再如,对于涉及多中心临床试验(或前临床实验)的企业,可能需要在全球范围内收集和处理受试者的信息,由此也同样会面临个人信息出境的情况,因此需要按照《个保法》的规定,满足个人信息出境的合规要求。除此之外,对于跨国经营的企业而言,可能需要将境内员工的个人信息传输至境外总部进行集中管理,在此场景下,企业不仅需要建立一套相应的流程向员工履行告知义务并征得他们的同意,还需要建立内部风险评估程序以降低个人信息出境的合规的风险。

3. 合规建议

《个保法》已经正式生效，虽然对于生命健康行业的相关企业而言，可能需要一定的时间来充分理解《个保法》并进一步采取相应的应对措施，但新规的执行并没有缓冲期，可以预见在不久的将来相关执法机构将开始进行规模化的检查执法。那么，对于生命健康行业的企业来说，应当采取哪些行动来积极应对并降低合规的风险？

(一) 建立内部的管理制度

首先，我们建议相关企业应当建立一套有效的内部的管理制度以保护个人信息，需要至少包括以下几个方面：(1)与个人信息管理有关的政策，其中应当涵盖《个保法》规定的相应内容；(2)设立负责个人信息保护的部门或专门人员；(3)对员工进行定期的培训以提高其对个人信息的保护意识和合规意识。上述管理制度的建立，一方面将有助于降低企业数据泄露的风险；另一方面可以在未来个人信息事件中被执法检查时作为一种有效的抗辩，证明企业已经采取必要的措施来保护个人信息。若企业因个人信息事件被起诉，相关个人信息管理制度以及对制度执行的内部记录将作为企业自证“无过错”的初步证据。

(二) 内部审计

其次，我们建议企业开展定期的内部审计活动。内部审计有两个主要目的：其一，可以帮助企业及时发现在执行《个保法》时存在的问题与疏漏；其二，可以根据企业对《个保法》的执行情况以及对内部管理制度的实施情况形成定期的记录。鉴于《个保法》对涉及个人信息处理活动的各个方面都提出了严格的要求，定期的内部审计将有助于企业及时发现问题并采取补救措施，如果相关内部审计能够证明企业在各方面都遵守了《个保法》，那么当企业陷入个人信息事件调查或相关的民事诉讼中时，内部的审计记录可以作为企业自证“无过错的”依据，以避免承担不利的法律后果。

(三) 重整业务流程

最后，我们建议相关企业可以考虑根据《个保法》要求重新梳理自身的业务流程，以明确哪些业务环节需要涉及到对个人信息的处理，并厘清相关业务活动下的法律风险点。对于内部审计时发现的问题及时处理，并根据《个保法》的合规要求考虑重新设计业务流程。例如，在一般情况下，通过医院直接征求患者的同意来收集他们的信息往往存在困难，相关企业可以考虑通过建立患者关爱平台，提供增值服务，以吸引患者在平台注册，并进而通过该平台来征得患者个人的同意。再比如，对于涉及提供远程医疗服务的企业来说，可以考虑将区域信息中心转移到中国境内，以便在境内存储相关个人信息，从而降低个人信息跨境传输的合规风险。

如您希望就相关问题进一步交流，请联系：



杨 迅
+86 21 3135 8799
xun.yang@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

上海市银城中路 68 号
时代金融中心 19 楼
T: +86 21 3135 8666
F: +86 21 3135 8600

北京

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

深圳

深圳市南山区科苑南路 2666 号
中国华润大厦 18 楼
T: +86 755 3391 7666
F: +86 755 3391 7668

香港

香港中环遮打道 18 号
历山大厦 32 楼 3201 室
T: +852 2592 1978
F: +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



www.llinkslaw.com



Wechat: Llinkslaw

本土化资源 国际化视野

免责声明：

本出版物仅供一般性参考，并无意提供任何法律或其他建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

© 通力律师事务所 2021