漢坤津師事務所
HAN KUN LAW OFFICES

汉坤专递

融贯中西
务实创新

2016 年第 11 期 (总第 116 期)

新法评述

1、 《网络安全法》简评（作者：唐志华、张驰、孙冠绯）

2016 年 11 月 7 日，第十二届全国人民代表大会常务委员会第二十四次会议，通过了历经三审稿的《中华人民共和国网络安全法》（“**《网络安全法》**”）。《网络安全法》全文共七章、七十九条，自 2017 年 6 月 1 日起施行。

《网络安全法》适用于在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理。本文对《网络安全法》下的重要制度和亮点做了相关梳理和总结。

一、 强调网络空间主权和国家网络空间安全

随着互联网和信息技术的持续发展，国家网络空间主权面临严峻挑战。全球互联网环境表面风平浪静，实则暗涌波涛。网络空间安全已成为一项关乎国家主权、安全和利益的重大议题，全球范围内各国均在积极制定和构建维护网络空间安全方面的法律措施和监管体系。

以欧盟为例，欧盟最高司法机构欧洲法院于 2015 年 10 月作出判决，认定欧美 2000 年签署的关于自动交换数据的《安全港协议》无效；2016 年 4 月，欧洲议会通过了商讨近四年的《一般数据保护条例》，堪称史上最严格的个人数据保护条例；2016 年 7 月欧洲议会通过了《网络与信息安全指令》，标志欧盟层面首部网络安全法案正式出台。

在此背景下，我国于 2015 年 7 月通过了新的《国家安全法》，第一次明确“网络空间主权”概念。2016 年 7 月颁布的《国家信息化发展战略纲要》强调，在推进国家信息化建设过程中维护国家网络空间主权、安全和发展利益，并加快制定网络安全立法。

本次公布的《网络安全法》遵循了国家坚持网络安全与信息化并重的宏观发展思路，并在关键信息基础设施保护、网络信息安全、监测预警与应急处置以及法律责任等方面落实了相关规则和措施，尤其是在最终稿中追加针对境外主体的追责措施[1]，有利于增强网络空间主权的防御能力和威慑能力。

二、 实施网络安全等级保护制度

《网络安全法》要求实行网络安全等级保护制度[2]。建立安全等级保护制度并非《网络安全法》首次提出的新要求。

公安部、国家保密局、国家密码管理局、国务院信息化工作办公室等国家四部委在 2007 年制定《信息安全等级保护管理办法》第七条中，将信息系统的安全保护等级分为五级，信息系统运营、使用单位应当按照《信息系统安全等级保护实施指南》具体实施等级保护工作；信息系统建设完成后，运营、使用单位或者其主管部门应当选择符合该办法规定条件的测评机构，依据《信息系统安全等级

[1]《网络安全法》第七十五条，境外主体从事攻击、侵入、干扰、破坏等危害中华人民共和国的关键信息基础设施的活动，造成严重后果的，依法追究法律责任；国务院公安部门和有关部门并可以决定对该机构、组织、个人采取冻结财产或者其他必要的制裁措施。

[2]《网络安全法》第二十一条。

保护测评要求》等技术标准，定期对信息系统安全等级状况开展等级测评，并履行相应备案手续。

相关行业主管部门还在 2007 年《信息安全等级保护管理办法》的基础之上，出台了加强本行业信息安全工作的指引和规范，如教育部于 2009 年 11 月发布《教育部办公厅关于开展信息系统安全等级保护工作的通知》，要求高校及地市级以上教育行政部门三级以上的信息系统要在教育部教育管理信息中心和当地公安部门同时办理备案手续；卫生部于 2011 年 11 月发布《卫生行业信息安全等级保护工作的指导意见》，要求第二级以上（含第二级）信息系统，应当报属地公安机关及卫生行政部门备案。因此，属于特定行业的单位在其信息系统达到一定安全等级时，将归入公安部门和行业主管部门的双重监管之下。

此外，工业信息化部于 2010 年 1 月颁布的《通信网络安全防护管理办法》还要求中华人民共和国境内的电信业务经营者和互联网域名服务提供者，对本单位已正式投入运行的通信网络进行单元划分，按照各通信网络单元遭到破坏后可能对国家安全、经济运行、社会秩序、公众利益的危害程度由低到高分别划分为五级，并向电信管理机构履行相应的备案手续、落实安全防护措施和进行符合性测评。

《网络安全法》作为我国首部网络安全专门性法律，首次以法律形式要求国家实行网络安全等级保护制度[3]，但《网络安全法》并未明确网络安全等级制度所具体参照的办法和标准，所以在未来的实际操作上是沿袭目前公安部牵头、各行业主管部门辅助的双轨监管模式，还是会后续制定统一的网络安全分级管理办法，尚有待进一步观察。

三、 对关键信息基础设施实行重点保护

《网络安全法》引入了“关键信息基础设施”的概念，并在前述网络安全等级保护制度的基础之上实行重点保护。“关键信息基础设施”作为关乎国家安全和利益的战略性资源，其重要性无需多言，对“关键信息基础设施”在法律和制度层面进行重点保护乃是目前各国立法的大势所趋。

从一审稿到三审稿，“关键信息基础设施”的定义经历了一波三折的纠结过程。正式稿最终采用非穷尽式列举的方式对其进行了定义：“关键信息基础设施”是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施。关键信息基础设施的具体范围和安全保护办法由国务院制定。前述定义，一方面通过行业列举大体勾勒出“关键信息基础设施”的属性，另一方面也为国务院后续进一步界定“关键信息基础设施”的具体范围和制定安全保护办法保留了空间和灵活性。

《网络安全法》对“关键信息基础设施”主要采取了以下重点保护措施：

1) 第三十五条规定，关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查，同时在法律责任部分制定了对应罚则[4]。

[3]《网络安全法》第二十一条。

[4]《网络安全法》第六十六条。

值得注意的是，涉及关键信息基础设施的国家安全审查并非是在《网络安全法》被首次祭出，在 2015 年初公布《外国投资法（草案）》[5]中，对我国关键基础设施和关键技术的影响即被列为外国投资国家安全审查应当考虑的因素。“关键（信息）基础设施”之于国家安全的重大战略性意义得窥一斑。

2) 第三十七条明确了关键信息基础设施相关信息跨境传输原则，即关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

至此，《网络安全法》成为目前首部限制数据向境外传输的法律，但该等限制仅针对关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据。值得注意的是，在《网络安全法》二审稿中，限制向境外传输的信息范围是“个人信息”和“重要业务数据”，最终稿将后者改为“重要数据”，限制境外传输的信息范围无疑有所扩大。

四、 完善个人信息保护制度

1) 受保护对象范围扩大：相比早前发布的《网络安全法》二审稿，《网络安全法》删除了“公民”在“个人信息”前的修饰，进而扩大了受保护对象范围，即包括所有使用我国网络服务的境内外个人，从而避免 “非公民”个人信息保护的立法真空。

2) 个人信息定义：《网络安全法》第七十六条规定，个人信息指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。上述对于个人信息范围的定义比较宽泛，但是相比 2013 年颁布的《电信和互联网用户个人信息保护规定》，《网络安全法》未包含可单独或结合其他信息识别用户使用服务的事件、地点等的信息[6]。

3) 大数据开发应用：《网络安全法》第四十二条规定，网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。根据本条但书的规定，网络运营者似乎只要能对合法收集的个人信息进行脱敏处理以达到无法识别个人且不能复原的程度，那么对该等数据的处理和使用可不受个人信息保护规定的制约。由此可见，立法者有意从制度设计层面为大数据的应用留下可行性空间，以取得个人信息保护和公众利益之间的平衡。

4) 明确网络运营者的信息安全义务：《网络安全法》整合了已经实施的《电信和互联网用户个人信息保护规定》、《全国人民代表大会常务委员会关于加强网络信息保护的决定》、《网络交易管理办法》、《消费者权益保护法》和《规范互联网信息服务市场秩序若干规定》等法律法规中对于网络信息保护的规定。具体要求包括：公开收集、使用用户信息规则；按约定收集、使用信息；采取适当措施，以确保上述信息安全并阻止用户个人信息泄露、毁损或丢失；当发生或可能已发生信息，及时采取补救措施等。而对于个人发现网络运营者存在违法收集、

[5]《外国投资法（草案）》第四章。

[6]《电信和互联网用户个人信息保护规定》第四条。

使用个人信息，并要求予以更正时，网络运营者应当采取措施予以删除或者更正[7]。

另外，《网络安全法》第四十九条规定，网络运营者对网信部门和有关部门依法实施的监督检查，应当予以配合。但该条没有明确配合的限度和执法机关应当遵循的正当程序，从而在监督检查过程中可能会产生争议甚至诱发权力滥用。

5) 网络诈骗等违法行为惩治：《网络安全法》第四十六条规定，任何个人和组织应当对其使用网络的行为负责，不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。监管机关可以依据第六十七条，对上述违法犯罪活动实施者进行处罚。原二审稿并没有该等条款，《网络安全法》正式出台后增加的这一规定，体现了立法和监管机关对目前泛滥的电信诈骗、电商乱象的整治决心。

五、 法律责任

《网络安全法》在二审稿基础上修改了部分处罚措施，将针对部分违法行为的罚金提高到原来的两倍。而对于从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动，或者为上述活动提供服务的行为，差别化适用行业禁入惩戒措施：受到治安管理处罚的人员，五年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作[8]。

六、 其他亮点归纳

1) 关注未成年人保护：《网络安全法》第十三条要求研究开发利于未成年人健康的网络产品和服务，惩治利用网络危害未成年人身心健康的活动，并配套规定了相应罚则，旨在为未成年人提供安全、健康的网络环境。

2) “网络运营者”定义：《网络安全法》根据第七十六条的规定，“网络运营者”指网络的所有者、管理者和网络服务提供者。这一定义范围较广，几乎囊括了利用网络开展活动的各类主体，也就是说在我国境内提供或者利用通信网络、互联网络等提供产品与服务的各类营利性与非营利性主体，都属于《网络安全法》监管范围。

3) 实名制认证：《网络安全法》第二十四条提出实名制认证要求，规定为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。相关网络服务提供者、网络运营者应注意严格遵守相关规定和标准。

4) 监管部门保密和合规使用义务：监管部门在相关日常监管、违法行为查处等活动中会接触到大量信息，因此《网络安全法》第三十条要求，有关部门在“履行网络安全保护职责”中获取的信息，只可用于维护网络安全需要。

另外，《网络安全法》第十四条规定了违法行为举报相关事宜，并要求有关部门对举报人信

[7]《网络安全法》第四十至四十五条。

[8]《网络安全法》第六十三条。

息予以保密，以保护其合法权益。这也是立法鼓励良性举报，促进社会监督的体现。

5) 监测预警与应急处理：网络安全的保障应当从事前预警、事中防范以及事后处置三个方面进行规范。《网络安全法》要求网络运营者应当制定网络安全事件应急预案[9]。另外，第五章专章规定网络安全监测预警和应急处理制度建设，要求建立国家层面的网络安全监测预警和信息通报制度，强化网络安全事件风险防范机制，健全网络安全事件处置机制，并引入《中华人民共和国突发事件应对法》、《中华人民共和国安全生产法》等有关法律、行政法规。[10]

结语：

《网络安全法》是我国第一部网络安全专门性法律，其以法律形式提纲挈领地整合了众多相关下位法中对网络安全、信息保护的规定，并契合大数据、信息化发展的大背景，具有重要的里程碑意义。过去我国网络安全事件、信息泄露事件时有发生，一个重要原因在于立法缺位和执法不严。违法成本不高、处罚力度不大，导致网络运营者未对网络信息保护给予足够重视并采取充分的安全保护措施。

近年来，我国政府愈发重视网络安全监管，注重个人信息保护。因此，我国境内企业，不论是网络所有者、管理者还是广大的网络产品、服务提供者，都应当严格遵守《网络安全法》的要求，认真落实网络安全保护和用户个人信息保护。同时，《网络安全法》的完善还有待在实践中总结经验，进一步制定与之配套的法律、法规、管理办法和标准等，我们将持续关注相关规定的后续发展。

==========

2、 健康医疗大数据领域的政策和法律问题（作者：朱敏、张驰）

随着云计算、物联网技术的持续发展，互联网日益加深对医疗健康产业的渗透乃至重塑。在此契机下，医院的信息化建设得到有效推进，移动医疗产业也呈现出迅猛发展的势头。互联网技术与医疗健康产业的日益融合，空前扩大了医疗数据的规模，于是越来越多的企业开始关注并积极探索健康医疗大数据的深度挖据和应用。

在此背景下，2016 年 10 月 25 日中共中央、国务院印发了《“健康中国 2030”规划纲要》。“健康中国 2030”是我国未来 15 年推进健康中国建设的行动纲要，其中特别强调发展健康产业和医疗大数据、培育健康医疗大数据应用新业态。由此可见，在国家政策的引导和激励下，医疗大数据有潜力成为未来健康医疗产业发展新的增长极。但与此同时，纲要也明确指出，需加强健康医疗大数据相关法规和标准体系建设。

目前，健康医疗大数据领域的法律法规存在明显的滞后性，因缺乏全面、细致、明确的指引和规则，健康医疗大数据的发展受到严重制约。虽然很多民营企业和外资企业都已迫不及待投身该领域并希望进行深耕布局，但受制于市场准入和产业政策的不确定性，目前尚在摸着石头过河，市场热情和

[9] 《网络安全法》第二十五条。

[10]《网络安全法》第五章。

活力并未得到充分、有效的释放。

本文旨在对健康医疗大数据领域可能涉及到的相关政策和法律问题进行了简要梳理和探究，供业界人士参考、拍砖。

一、 健康医疗大数据的概念

“大数据”与“云计算”、“物联网”一样，均是近些年来伴随着新一轮产业革命的深入发展而涌现出来的新名词。根据 2015 年 8 月国务院《促进大数据发展行动纲要的通知》，“大数据”是以容量大、类型多、存取速度快、应用价值高为主要特征的数据集合。“健康医疗大数据”无非是“大数据”下属的一个分支，专注于“健康医疗数据”的集成和应用。

国家卫计委 2014 年在《人口健康信息管理办法（试行）》对“人口健康信息”进行了定义：人口健康信息是指依据国家法律法规和工作职责，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。参照前述“人口健康信息”的定义，“健康医疗数据”应该主要是指个人免疫、体检、门诊、住院等健康活动所产生的数据。不过，随着可穿戴设备等物联网智能产品的普及，广义上的“健康医疗数据”还可延伸至个人使用健康医疗移动应用而产生的数据。

二、 健康医疗大数据的价值和国家宏观政策

健康医疗大数据是一种高附加值的信息资产，虽然个体健康医疗数据对于医疗技术革新的价值有限，但通过对海量、来源分散、格式多样的数据进行采集、存储、深度学习和开发，可以从中发现新知识、创造新价值、提升新能力，从而进一步反哺健康医疗服务产业。因此，健康医疗大数据的发展关乎国计民生，具有重大的战略性意义。

目前，国家已陆续出台关于扶持医疗大数据发展的相关政策，初步做好顶层设计并构建出医疗大数据发展的宏伟蓝图：

1) 2014 年国家卫计委制定“46312”工程，即建设国家级、省级、地级市、县级 4 级卫生信息平台，依托于电子健康档案和电子病历，支撑公共卫生、医疗服务、医疗保障、药品管理、计划生育、综合管理等 6 项业务应用，构建电子监控档案数据库、电子病历数据库、全员人口个案数据库 3 个数据库，建立一个安全的卫生网络，加强卫生标准体系和安全体系建设。

2) 2015 年，第十二届全国人民代表大会上李克强总理提出制定“互联网+”行动计划，“互联网+医疗行业”进一步推动互联网与传统医疗行业的融合。

3) 2016 年 6 月，国务院办公厅关于《促进和规范健康医疗大数据应用发展的指导意见》中指出，将推动健康医疗大数据资源共享开放。

4) 2016 年 10 月 22 日，为推进和规范健康医疗大数据的应用发展，福建省、江苏省及福州、厦门、南京、常州被确定为健康医疗大数据中心与产业园建设国家试点工程第一批试点省市。

5) 2016 年 10 月 25 日，中共中央、国务院印发了《“健康中国 2030”规划纲要》，其中特别提到加强健康医疗大数据应用体系建设，推进基于区域人口健康信息平台的医疗健康大数据开

放共享、深度挖掘和广泛应用。

三、 发展健康医疗大数据面临的现实障碍

虽然在宏观政策层面国家对于发展健康医疗大数据是鼓励和扶持的，但是具体到政策落地和具体操作，尚有多项现实性难点和障碍需要攻克和破除，主要包括：

1) 健康医疗大数据的共享和开放程度不高

医疗卫生机构无疑是采集和存储健康医疗大数据的主力军，而且相比较基于移动医疗应用所产生的数据，源自医疗卫生机构的数据特别是电子病历数据(EMR)，具有更高的准确度和商业开发价值。但是在目前的医疗体制下，医疗卫生机构很难有动力去共享这些数据，医疗卫生机构和医疗卫生机构之间、医疗卫生机构和社会公众领域之间，均存在不同程度的数据壁垒。数据孤岛效应一方面造成了患者数据重复采集和医疗资源浪费，另一方面也阻碍了健康医疗大数据的系统性开发和建设。

随着医疗体制改革的深入和医院信息化程度的提升，院际之间的数据壁垒有望被进一步打破。国务院办公厅在《促进和规范健康医疗大数据应用发展的指导意见》中指出，建立跨部门密切配合、统一归口的健康医疗数据共享机制；《“健康中国 2030”规划纲要》提到，要消除数据壁垒，建立跨部门跨领域密切配合、统一归口的健康医疗数据共享机制，实现公共卫生、计划生育、医疗服务、医疗保障、药品供应、综合管理等应用信息系统数据采集、集成共享和业务协同。

由此可见，未来在政府牵头和多部门协调配合下，健康医疗大数据的应用会得到系统性开发和建设，院内数据孤岛状况有望进一步改善甚至根本性破除。但是，未来该等医疗数据资源是否会向民营企业和外资企业开放以及可能开放的程度，目前尚未可知。另外，建设全国健康医疗数据资源集成和共享平台涉及多方监管部门和参与主体，实施起来存在较大难度，距离平台最终建设完成乃至进一步开发和利用可能还有很长一段路要走。在此期间，民营企业和外资企业可能只能通过开展双边合作的形式使医疗卫生机构共享数据资源，小心翼翼的探索健康医疗大数据的开发和应用。

2) 健康医疗大数据领域的法律体系亟待完善

关于健康医疗数据的权属：目前的法律体系尚不能很好的解释和界定健康医疗数据的权属问题，特别是医疗数据的所有权，导致实践中存在健康医疗数据的所有权到底属于患者个人还是医院的争议。有观点认为，医院和患者均参与到医疗数据的形成，因此理论上健康医疗数据是属于大家的；还有观点认为，医疗数据的所有权在于患者个人、控制权在于医院、管理权在于政府，第三方机构需借助政府支持和医院配合方能对其进行商业化开发和利用。健康医疗数据权属的模糊性，一方面掣肘着健康医疗数据的授权使用，另一方面也给患者的个人信息权保护提出难题并埋下了隐患。

健康医疗大数据作为一种信息资产，在现行的法律框架下，如果医疗机构或经授权的第三方机构对数据进行了合法处理从而使其具有了智力成果或经济价值属性，那么该等数据可以在知识产权或商业秘密的框架下予以保护；对于医疗机构和移动医疗运营商采集的与个人医疗

健康相关的原始信息和数据，主要还是属于个人信息和隐私的范畴，可从人身权维度进行保护。

关于个人数据的法律保护：目前围绕个人信息保护的立法正稳步开展并趋向完善：目前尚在审议中的《民法总则》草案有望将个人信息权从隐私权中独立出来，专门进行保护；随着公民个人信息权利意识的提高，立法机关可能会加快制定和出台个人信息保护单行法的进程；《网络安全法》三审稿已于今年 10 月公布，有望年底或明年出台。

值得注意的是，《网络安全法》二审稿第四十一条规定，“网络运营者不得泄露、篡改、毁损其收集的公民个人信息；未经被收集者同意，不得向他人提供公民个人信息。但是，经过处理无法识别特定个人且不能复原的除外”。根据本条但书的规定，大数据应用必须对公民个人信息进行无法识别特定个人处理。换句话说，数据控制人只要能对合法收集的个人信息进行脱敏处理以达到无法识别个人且不能复原的程度，那么对该等数据的处理和使用可不受公民个人信息保护规则的制约。由此可见，立法者有意从制度设计层面为大数据的应用留下可行性空间，以取得个人信息保护和公众利益之间的平衡。

四、 发展健康医疗大数据的法律合规性建议

虽然在宏观政策层面健康医疗大数据的发展是受引导和鼓励的，但由于法律的滞后性目前尚缺乏系统、细致的规则给与指引和规范。尽管如此，我们基于对行业实践的观察并结合当前的立法趋势，简要梳理总结了如下法律合规性建议以供参考：

1) 规范健康医疗数据的采集活动：

(1) 如是通过自身或关联公司开发的平台收集健康医疗数据，总体上须遵循合法、正当、必要的原则，并通过 Privacy Policy 或其他方式明示收集、使用信息的目的、方式和范围，且经被收集者同意；

(2) 如是依赖医疗卫生机构共享医疗数据，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。

值得关注的是，欧盟于 2016 年 4 月通过了《一般数据保护条例》（General Data Protection Regulation），在这部堪称史上最严格的数据保护条例中，规定了个人数据处理的透明性（Transparency）、最少数据收集（Data Minimization）原则，并赋予数据主体随时撤销同意权（Right to Withdraw Consent）、被遗忘权（Right to Erasure）、可携带权（Right to Portability）等权利。

虽然目前中国法下尚未明确规定该些原则和创设该些权利，但是随着个人信息保护立法进程的深入推进和经济全球化进程的日益加深，相信中国会越来越多的借鉴和参照发达国家在个人信息立法方面的经验和水平，所以在此提示关注并建议合规标准较高的跨国企业可以考虑比照适用。

2) 数据本地化存储及境外传输：在目前强调网络空间主权的形势下，须做到在中国本地化存储健康医疗大数据，并在无法肯定对外输出数据明显不构成危害国家安全、国计民生和公共利

益的情况下，尽量避免向境外传输具有一定敏感度的健康医疗数据。

目前在法律层面，尚不存禁止向境外输出健康医疗大数据甚至是个人信息数据的规定。之前在制定《反恐怖主义法》时，草案曾试图要求电信和互联网服务提供者应当将相关设备和境内用户数据留存在境内的要求，但因争议较大，2015 年 12 月 27 日正式颁布的版本中最终删除了该项规定。不过需要注意的是，目前公布的《网络安全法》二审稿中引入了“关键信息基础设施”的概念，并限制关键信息基础设施的运营者将在中国境内存储在运营中收集和产生的“公民个人信息”和“重要业务数据”传输至境外。如果健康医疗数据处理平台属于关键信息基础设施的范围，则向境外输出该平台上收集和存储的“公民个人信息”需经相应的安全评估方能实施，而且即便能通过技术手段可以做到数据不再具有“公民个人信息”的特征，但该类数据还是有可能落入“重要业务数据”的范畴，从而在向境外输出时将受到同样严格的限制。

在规章层面，国家卫计委在其颁布的《人口健康信息管理办法（试行）》明确禁止将人口健康信息存储在境外服务器上。但严格意义上说，该等限制应仅局限于人口健康信息，即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，应该不适用于基于健康医疗移动应用而采集到的一般个人健康信息和对人口健康信息进行脱敏处理后而产生的数据。

3) **完善安全保护技术措施**：健康医疗大数据平台运营商应采取技术措施和其他必要措施，确保信息安全，防止在业务活动中收集的涉及公民个人信息发生数据泄露、毁损、丢失的情况。在发生或者可能发生信息泄露、毁损、丢失的情况时，应当立即采取补救措施。此外，数据安全保护措施还需达到相应标准。《网络安全法》二审稿规定国家将实行网络安全等级保护制度。网络运营者应当建立内部合规系统，根据不同的安全等级履行安全保护义务。

其实，建立安全等级保护制度并非是《网络安全法》首次提出的新要求，公安部、国家保密局、国家密码管理局、国务院信息化工作办公室等国家四部委在 2007 年制定《信息安全等级保护管理办法》第七条将信息系统的安全保护等级分为五级，信息系统运营、使用单位应当按照《信息系统安全等级保护实施指南》具体实施等级保护工作；信息系统建设完成后，运营、使用单位或者其主管部门应当选择符合该办法规定条件的测评机构，依据《信息系统安全等级保护测评要求》等技术标准，定期对信息系统安全等级状况开展等级测评，并履行相应备案手续。

在此基础之上，卫生部于 2011 年在《卫生行业信息安全等级保护工作的指导意见》的通知中指出，国家信息安全等级保护制度将信息安全保护等级分为五级：第一级为自主保护级，第二级为指导保护级，第三级为监督保护级，第四级为强制保护级，第五级为专控保护级。重要卫生信息系统安全保护等级原则上不低于第三级。

鉴于健康医疗大数据平台处理数据的范围和在此基础之上的应用开发主要涉及或着眼于医疗卫生行业，建议参照卫生部在《卫生行业信息安全等级保护工作的指导意见》的相关规定和标准建立和落实相关数据安全等级保护制度。

4) **健康医疗大数据领域的外资限制**：目前政策层面尚不存在限制或禁止外资参与健康医疗大数

据领域的直接规定。但如果采集和处理的数据涉及人类遗传资源，则按照《人类遗传资源管理暂行办法（1998）》以及《人类遗传资源采集、收集、买卖、出口、出境审批行政许可事项服务指南（2015）》，与外方或外商投资企业合作采集人类遗传资源或将其传输至境外需由科技部批准之后方能实施。

医疗健康大数据领域的外资限制还可能体现在健康医疗大数据平台的运行方式和具体的业务结构层面，例如跨国公司通过设立专业医疗机构方式布局健康医疗大数据领域，则会受到外商投资医疗机构的政策限制；如果跨国公司通过云平台、物联网平台或是基于区块链技术的 BaaS 平台采集和处理健康医疗大数据，可能还会涉及外商投资增值电信领域的限制；此外，跨国公司拟与医疗卫生机构就健康医疗大数据开展合作时，也可能遇到医疗卫生机构倾向和非外资方开展合作的隐性商业壁垒。

总而言之，从事健康医疗大数据开发和应用是否存在以及存在何种外资限制，目前尚不能一概而论，需在具体项目中综合所涉及的数据范围、数据平台的运作方式以及具体的业务结构进行分析和判断。

特别声明

汉坤律师事务所编写《汉坤专递》的目的仅为帮助客户及时了解中国法律及实务的最新动态和发展，上述有关信息不应被看作是特定事务的法律意见或法律依据，上述内容仅供参考。

如您对上述内容有任何问题或建议，请与汉坤律师事务所的下列人员联系：

联络我们

北京总部
电话：+86-10-8525 5500
地址：中国北京市东长安街 1 号东方广场办公楼 C1 座 9 层
邮编：100738

陈容 律师：
电话：+86-10-8525 5541
Email：estella.chen@hankunlaw.com

上海分所
电话：+86-21-6080 0909
地址：中国上海市静安区南京西路 1266 号恒隆广场 5709 室
邮编：200040

曹银石 律师：
电话：+86-21-6080 0980
Email：yinshi.cao@hankunlaw.com

深圳分所
电话：+86-755-3680 6500
地址：中国深圳市福田中心区中心四路 1-1 号嘉里建设广场第三座 21 层 03 室
邮编：518048

王哲 律师：
电话：+86-755-3680 6518
Email：jason.wang@hankunlaw.com

香港分所
电话：+0852 2820 5600
地址：中国香港中环夏悫道 10 号和记大厦 20 楼 2001-02 室

陈达飞 律师：
电话：+0852-2820 5616
Email：dafei.chen@hankunlaw.com