OMAHA
Open Medical and Healthcare Alliance
开放医疗与健康联盟
漢坤津師事務所
HAN KUN LAW OFFICES

OMAHA白皮书

WHITEPAPER

2017 年 01 月　第 3 期

www.omaha.org.cn

如何保护个人健康医疗信息?

How to Protect Personal Health Information?

敬请关注
OMAHA官方微信

敬请关注
汉坤官方微信

2017 年 01月 第 3 期

”大数据的商业应用已经无处不在，但几乎没有人关心被提取数据人的权益。“

—— 涂子沛 大数据专家、OMAHA基金会理事长

目 录

内容摘要

随着大数据、云计算、人工智能、物联网、传感器等技术的兴起与成熟，健康医疗信息的应用价值在加强卫生医疗行业管理，辅助公共卫生监测评估和决策管理，提高医学研究和临床疾病诊疗质量和促进个人自我健康管理能力等方面得到了更大体现。

由于健康医疗信息应用价值的提升，产生了更多对个人健康医疗信息保护的需求。个人健康医疗信息保护面临着信息的互联网化、个人信息量的增大、个人信息的接触者增多和数据身份还原技术增强等新的挑战。

(一) 个人健康医疗信息的定义

在本白皮书中，我们将“个人健康医疗信息”定义为：能够识别出个人身份的所有健康医疗相关信息，包括各级各类医疗卫生计生服务机构产生的人口健康信息，和可穿戴设备、智能健康电子产品、健康医疗移动应用、网络在线平台等产生的个人健康医疗相关的信息。

(二) 国外对个人健康医疗信息的保护

欧盟和美国都对个人健康医疗信息进行了立法保护，且在近十年中都因互联网技术的迅速发展，颁布了新的法律以适应新的情景和需求。其中主要有美国 2003 年生效的 HIPAA 隐私规则和安全规则、2013 年生效的 HITECH Omnibus Rule 以及欧盟 2015 年颁布的《一般数据保护条例》。

由于法律体系和医疗健康产业发展过程的不同，美国和欧盟法律对于个人健康医疗信息的保护在立法体制、覆盖主体、保护范围和“公共利益”议题上都出现了较大差异，但美国法律赋予个人关于健康医疗信息的隐私权与欧盟法律中体现的个人信息权的具体内容非常相似：都强调个人对于自己的健康医疗信息拥有支配权、决定权和控制权。

(三) 我国对个人健康医疗信息的保护

我国不仅在法律法规体系建设方面已经完成了基本的框架搭建，在健康医疗领域的相关立法和政策布局工作也取得了很多进展，包括国家和地方层面出台了一系列的政策和指导意见。而《网络安全法》的颁布，以及目前仍处于立法进程中的《民法总则》将个人信息保护纳入权利保护框架的动议，将我国的个人信息保护的立法制度建设提高到了一个新的高度。

但对比美国和欧盟的相关立法，我国针对个人健康医疗信息的法律规定上还存在个人信息权定位不明、法律法规不成体系、内容较为单薄和处罚力度不足等问题。

(四) 倡导和建议

为了维护个人权益，推动健康医疗大数据行业的有序发展，我们针对政府、医疗机构、商业机构和个人提出了以下建议：政府能够制定专门法律明确个人信息权的定位，赋予个人更多关于个人健康医疗信息的权利，根据具体需求制定更详细法规明确实施细节和救济方法；医疗机构需要形成行业内的电子健康信息交换标准以促进信息的可携带性和可交换性，加强对相关商业机构的约束，促进个人健康医疗信息权益的实现；相关商业机构了解并遵守国内外相关法规，合法采集、接入、存储和使用个人健康医疗信息；个人应当增加法律意识，维护个人健康信息权益。

研究简介

(一) 研究背景

近年来，随着医疗信息化和互联网技术的不断发展，电子结构化的健康医疗信息数据量迅速增长，应用价值不断提升。而信息技术的发展也为个人健康信息权益保护带来了种种新的挑战，个人信息保护的法制建设日益得到个人和行业的广泛关注。

(二) 研究目标

在此背景下，基于国内个人健康医疗信息权益保护的现状和需求，我们研究了国际上一些代表性国家和地区的个人健康信息权益保护的法律法规，希望通过横向对比和分析借鉴，对政府立法、医疗机构及商业机构合规和个人维权进行建议。

本文只探讨对个人健康医疗信息保护在法制层面的建设和行业层面的应用，不涉及国家领导机构设置和其他相关措施；本文不对配套的具体信息保护安全措施展开详述。

(三) 研究方法

本文通过文献检索和相关资料查询对国内外有代表性和参考价值的个人健康医疗信息保护的法律法规进行了归纳和研究；同时选取国内具有代表性的行业机构，例如医疗信息技术服务商、医疗机构、基因检测服务商等，并与从业人员进行深度访谈，调研了国内相关机构或人员对于健康医疗信息保护的理解和需求，对比了国内外立法状况的差距，提出促进行业有序规范发展的相关建议。

(四) 开放医疗与健康联盟

开放医疗与健康联盟（Open Medical and Healthcare Alliance，OMAHA）是一个致力于推动产业开放个人健康医疗数据的非政府组织（non-government organization，NGO），希望通过协作定义个人健康档案的标准格式，探索相关信息标准的落地，从而提高老百姓对自身健康医疗数据使用的完整性、可及性和可用性，以推动医疗、健康产业信息开放、共享、开源。

(五) 汉坤律师事务所

汉坤律师事务所自 2004 年成立以来，已迅速成长为中国领先的综合性律所之一。全球化背景下，汉坤一直专注于服务生命科学与健康领域，以使其始终处于中国律师行业的最前沿。汉坤生命科学与健康团队尤其以公司合规监管、反垄断和竞争法、劳动、知识产权、诉讼、私募股权、兼并和收购等领域的法律服务著称。汉坤连续被钱伯斯、China Law and Practice 等国际知名法律媒体评为生命科学和健康领域的杰出中国律所。

此白皮书的发布旨在与业界分享 OMAHA 在推动健康医疗数据开放事业的同时，对个人信息的保护相关的研究成果，呼吁行业加快对数据利用和价值挖掘的过程中，兼顾对个人健康医疗信息的保护，同时推动这部分特殊信息在我国法治层面的管理和保护。在白皮书的撰写过程中，特别感谢汉坤律师事务所的专业支持，与 OMAHA 一同推动对个人健康医疗数据的保护，为生命健康产业的有序发展贡献一份力。

一、 健康医疗信息的价值和挑战

(一) “健康医疗+互联网”背景下个体数据的巨大利用价值

随着互联网浪潮的来临，大数据、云计算、人工智能、物联网、传感器等技术的兴起与成熟，个人信息被称为“新石油”，个人信息交易已形成一定规模。根据欧洲司法专员 Viviane Reding 的预计，到 2020 年个人数据交易将占欧洲 GDP 总量的 8%，成为名副其实的数字经济的货币。

在健康医疗领域，健康医疗信息也正以指数级的速度爆炸式地增长，可用的数据越来越多；信息不再只是零散地储存在病案和就医记录等文书中，转而以结构化电子信息的形式进行储存和传输，为数据的快速采集提供了便利条件[1]。同时，健康医疗信息的应用价值不断提升，更趋于多元化。2016 年 6 月，国家卫生和计划生育委员会发布《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，鼓励集成医疗大数据平台，构建临床决策、疾病诊断、药物研发等支持系统，拓展公共卫生监测评估、传染病疫情预警等应用；重点推进网上预约分诊、检查检验结果共享互认、医保联网异地结算等便民惠民应用，发展远程医疗和智能化健康医疗设备[2]。

可以说，是这个时代赋予了这些健康医疗信息更多的生机和活力转变。利用大数据技术可以从中发现潜在的关系、模式，从而帮助医师提高诊断精度、预测治疗效果、降低医疗成本，帮助医药公司发现潜在的药物不良反应、帮助公共卫生部门及时发现潜在的流行病等。基于不同场景，无论是基于个体还是群体，通过信息的挖掘、分析、验证来满足对数据再利用的需求也越来越强烈，具体可归纳为如下主体提供价值和服务：

1. **政府：帮助加强卫生医疗行业管理，提升公共卫生监测评估和决策管理能力。**
   - **有利于管理部门对医疗行业更有效的监管。**传统上，政府对医疗机构及整个行业的管控，大多是基于零散保存于各个医疗机构的处方、病历资料，政府监管失灵时有发生；而目前，管理机构将越来越多地通过对健康医疗信息资源的整合与共享，更高效地调用医疗机构内部的数据，并实时在网络上监测医疗机构发生的医疗行为，提高政府管理水平。例如，电子病历的应用撬动了医保监管和控费审核模式的改革。医保部门通过医疗数据分析及医保精准控费，实现各地医保基金的统筹管理，保证医疗服务方的服务质量。
   - **帮助公共卫生监测。**随着人们生活和行为方式的改变，新发传染病已成为公共卫生领域的严峻挑战。利用新的技术和方法来提高疾病发现、追踪、报告和响应也应运而生，例如整合社会网络公共信息资源，利用公众健康医疗相关数据进行智能分析来提高突发公共卫生事件预警与应急响应能力。2009 年，Google 比美国疾病控制与预防中心提前 1-2 周预测到了甲型 H1N1 流感爆发，此事件震惊了医学界和计算机领域的科学家。Google 正是借助大数据技术从用户的相关搜索中预测到流感爆发。虽然，由于数据收集的方法欠缺精准性，导致之后多次出现 Google 疫情误报的报道，但其在流感预测方面的尝试或许能够成为利用大数据造福社会的一个好的模式[2]。

2. **临床：医学研究和临床疾病诊疗的提升有赖于健康医疗数据的高质量汇聚和挖掘。**
   - **辅助临床决策支持，提高诊疗水平。**医生在对患者进行诊断和治疗等行为的过程中需获取、了解、使用的患者健康数据量越来越大，但在整个长期的诊疗过程中，医

生往往难以掌握患者全部的健康医疗信息，由此带来的结果可能是医疗差错或治疗效率较低。目前，部分省市的医疗机构可通过区域平台来集成患者的健康信息，包括患者历次体征、既往病史、治疗方案和治疗效果等信息，帮助医生评估在实际临床应用中的疗效进而提供最佳的治疗方法。另一方面，高质量的医疗数据可以应用于临床决策支持系统，分析医生输入的医嘱，比较其与医学指南的差异，并进行知识转化，提醒医生防止潜在的错误，从而降低医疗事故率。以 IBM Watson 为代表的临床决策系统在开发之初只是用来进行分诊的工作，到了 2011 年，Watson 开始协助医生进行临床决策。此前，通过与 Memorial Sloan-Kattering 癌症研究中心、克利夫兰诊所（Cleveland Clinic）等医疗机构的合作，Watson 系统已经具备了学习并分析已有的病历、治疗、用药等方面信息的能力。可以预见，未来人工智能和互联网、大数据等其它先进技术将成为医生的得力助手[3, 4]。

- **提升临床医学研究的质量。**临床研究主要以疾病的诊断、治疗、预后、病因和预防为主要内容，以患者为主要研究对象，需要大量的临床数据作为研究基础。[5]医疗机构主要的数据来源为医院信息系统（Hospital Information System，HIS）大量存留的患者临床诊治过程数据，是个人健康医疗信息的重要组成部分。相对来说，这些数据医学专业程度及结构化程度较高，反映了患者真实的就医过程，包涵了有待发掘和利用的医学价值。在互联网背景下，医院内部数据的结构化程度加强，数据传输及汇集变得简单有效，大数据相关的计算机技术、数据分析、数据挖掘方法的发展也使面向医疗数据的临床深度研究成为可能。因此，医生及科研人员从临床病历信息中提取有效数据的效率、数据的精准性都在不断提升。

3. **个人：健康医疗信息的利用能充分发挥个人在全程健康管理中的能动作用。**
   - **提高患者在诊疗过程中的参与度。**在过去，由于医患双方信息的不对称、患者健康素养普遍较低，患者对自身疾病状况和健康状态往往知之甚少，可以说患者是整个医疗过程中最未被充分利用的资源。而随着我国公众健康意识的不断提升，个人可获取健康疾病知识的途径趋于便捷与多样化，越来越多的患者将意识到“个人是其健康的主体”。当患者掌握完整的医疗信息，对自我健康状况充分知情，才能提高其在健康、医疗、养老方面的参与度和积极性，充分发挥患者在医疗就医和养老护理过程中的能动作用。
   - **加强个人对自身的日常健康管理。**随着互联网的发展，医疗技术更倾向于互联化、一体化，这也使得大量的丰富的由个人产生的健康数据变得易于获取，如各种移动设备、应用程序、健康服务（如用户基因检测服务）等。以人体健康为诉求的移动健康设备及智能可穿戴式设备已经走进人们的生活，用户可以通过可穿戴式智能设备随时随地采集自身体征数据，实现对个人健康状况的不间断监控，通过获得的生理参数和运动参数加强自我健康管理。
   - **利用基因数据进行疾病预测。**随着基因检测技术包括全基因组测序的普及，人们的个性化需求将会被精准细分，基因信息可以帮助个体选择更好的医疗决策方案。美国女星安吉丽娜朱莉就是通过基因检测发现携带突变的 BRCA1 基因，患乳腺癌的风险高达 87%，患卵巢癌的风险为 50%，因此她选择切除了乳腺、卵巢和输卵管。[6]如今越来越多的人渴望得到个体的基因数据，成为自身遗传数据的管家。

4. **产业：健康医疗大数据资源共享开放，可培育数据应用的新业态。**

- **协助开展临床药物研发和药物警戒研究。**医疗信息数量大，医疗信息的整合可以衍生出多种医疗层面高价值的应用和模式。一方面，在医药产品研发上，制药公司可以通过对数据的挖掘有效判断研发项目成功的可能型，以供支持更高效的药物临床试验项目。再如，在药物警戒领域，传统的药物副作用分析主要采用临床试验法、药物副作用报告分析法等，普遍受制于样本数小、采样分布有限等因素影响，难以全面反映药物副作用。自上世纪 90 年代以来，政府追踪药物不良反应（涉及患者、医生、医药公司）的流程并未发生太大改变，因此，药物安全监测的速度也会比较慢。随着医疗大数据库系统的应用，可从千百万患者的数据中挖掘到与某种药物相关的不良反应，样本数大，采样分布广，所获结果更具有说服力。美国 FDA 正与 Google 探讨如何借助后者的搜索引擎来寻找和确定某些药物以前并不为人所知的副作用。
- **实现精准医疗。**2015 年 1 月 20 日，美国总统奥巴马在国情咨文中提出“精准医学计划”。精准医疗强调在治疗时考虑个人的基因变化、环境影响、生活方式等，是近几年兴起的疾病治疗方案。近来，我国政府也提出了“精准医疗计划”：计划在 2030 年前，投入 600 亿到精准医疗领域。而作为精准医疗得以落地实施的基础，一方面，随着基因监测技术的成本趋于便捷与平价、不同来源的医疗健康数据以个体为承载对象进行汇集，各个信息平台积累足够的患者数据；另一方面，大数据分析的能力不断加强，基于大量的数据基础进行的分析将变得愈加精准，从而为个人的精准医疗提供帮助。

综上，对于个体来说，获得自身完整的健康医疗数据是对自我健康监测、管理、预防的基础；从整个医疗行业的发展趋势来看，未来将有更多利益相关者依赖日益庞大健康医疗数据。

(二) 个人健康医疗信息的保护遭遇空前挑战

在互联网上，一切的连接变得轻而易举。随着互联网在健康医疗领域的深入，数据的产生、采集、连接、利用能力得到提升，同时也产生了许多全新的与个人健康医疗信息保护相关的矛盾点。个人健康信息被非法窃取和被的现象时有发生：2014 年全国已出现多省市数千万用户医保信息泄漏的报道，如山东省疾控制中心某内部系统泄露近 190 万病人信息和近 140 万随访信息，江苏省疾控中心某平台漏洞导致几千万敏感信息被泄露、海南省卫生厅某系统漏洞可能泄露全省数千万参保人员及医疗报销人员详细敏感信息等。2014 年 2 月，英国 care.data 数据库中包含了 30 年 4700 万患者的信息被卖给保险公司[6]。IDC 市场研究公司在其 2015 Health IT 预测中多次提到，移动健康医疗现在拼的是产品，2018 年拼的是安全。在 2020 年，预计全球 42%电子健康数据会处于无保护状态，但它们需要被保护[7, 8]。

可见，移动互联网医疗、大数据技术的兴起，为大家创造价值的同时，也给个人健康信息保护带来了诸多挑战，以下几个因素大大提升了信息保护的难度：

1. 健康医疗信息的互联网化

近年，互联网在我国民众的工作、生活中迅速普及，网民上网设备也逐渐向手机端倾斜。2016 年 1 月 22 日，中国互联网络信息中心（CNNIC）发布了第 37 次《中国互联网络发展状况统计报告》称“截至 2015 年 12 月，中国网民规模达 6.88 亿，互联网普及率达到 50.3%，其中，2015 年新增网民 3951 万人，增长率为 6.1%，较 2014 年提升 1.1 个百分点，网民规

模增速有所提升。”《报告》同时指出“网民的上网设备正在向手机端集中，截至 2015 年 12 月，我国手机网民规模达 6.20 亿，有 90.1%的网民通过手机上网。只使用手机上网的网民达到 1.27 亿人，占整体网民规模的 18.5%”[9]。医疗健康领域也加入到了这股互联网应用热潮中：

- **原本沉寂在医院内网的健康信息，如今随着各机构门户网站的建立，医院内网与互联网相连，信息在互联网上流通起来，**患者可轻松通过互联网接入医院信息系统进行预约挂号、查询报告、缴费等操作。同时，多个省份区域卫生信息平台的建立也使得信息进一步可流动。《全国医疗卫生服务体系规划纲要（2015-2020 年）》提出，到 2020 年我国将实现全员人口信息、电子健康档案和电子病历三大数据库，基本覆盖全国人口，同时建成互联互通的国家、省、市、县四级人口健康信息平台[10]。截至 2016 年，全国已建成天津、辽宁、上海、江苏、浙江等 11 个基于居民电子健康档案的省级区域卫生信息平台；80 个市级及 485 个县级建设基于居民电子健康档案的区域卫生信息平台。其中，市平台与省平台的联通率为 71.97%，县（区）平台与上级平台的联通率为 45.31%。[11]
- **越来越多的健康医疗信息通过物联网、互联网产生。**随着移动物联网的兴起，患者借助各种各样的物联网医疗设备来产生自己的健康数据，并且分享给身边的医生、朋友、家人。据统计，2015 年，平均每个人连接的“物联网医疗设备”超过 3.47 台，预测到 2020 年，每个人连接的设备数量将超过 6 台；而在 2003 年，这个数字只有 0.03 台。患者对“物联网医疗设备”的需求不断增长，刺激了全球越来越多的“物联网医疗设备”产生：据 Intelligence 预测，2018 年全球可穿戴设备出货量将达 3 亿台，全球可穿戴设备销售规模将达到 120 亿美元。另据预测，到 2020 年，我国可穿戴医疗设备市场规模将有望接近 260 亿元人民币[10]。同时，在线的医疗医药服务平台也迅猛发展，产生了大量的“增量”数据。线上医疗服务主要包括在线挂号、在线咨询、在线问诊、在线购药、远程医疗等，预计 2020 年 B2C 医药电商市场规模将达 746.83 亿元[10]。这些都意味着越来越多的健康信息在线上服务平台上产生。

2. 个人健康医疗信息量变大

丰富多彩的互联网医疗形态，使健康医疗数据的生成来源也多样化：HIS、电子病历系统（EMR）、实验室信息管理系统（LIS）、医学影像管理系统（PACS）等信息系统产生的人口健康信息；在院外，医生经过移动端、电脑端对病人进行咨询、会诊、转诊等活动时形成的电子数据；可穿戴设备如血糖、血压、血氧检测仪等，大型自动化设备如 CT 仪、MRI 仪、B 超机、血透装置、各种管腔介入治疗仪、甚至是手术机器人等产生的数据；患者在网络购药过程中形成的交易数据等，个人的健康医疗数据激增。

2012 年 12 月 2 日，根据 IDC 市场研究公司撰写的《数字宇宙驱动医疗行业数据增长》报告揭示：医疗行业的数据量占比显著，每年以 48%的速度增长，是增速最快的行业之一。2011 年，单美国的医疗健康系统数据量就达到了 150EB。基因数据也是非常庞大的存在，一次全面的基因测序，产生的个人数据则达到 300GB。公开发布的基因 DNA 微阵列达到 50 万之多，每一阵列包含数万的分子表达值[12]。随着我国医疗卫生机构信息化程度不断提高，医院每天产生大量的电子健康医疗信息，大型医院每年的数据增量在数十 TB，仅医学影像每年可达 20TB[13]。移动医疗平台存储的健康数据量也相当惊人，如春雨医生目前已沉淀了 3000 万量级的医患问答数据，主要集中在妇科、儿科、皮肤科等[14]。

3. 个人信息的接触者更复杂

如前所述，区域卫生信息平台的建立，移动医疗、互联网医疗的兴起，使获取个人健康数据的渠道越来越丰富，也意味着更多的主体可以接触到患者的个人信息。如区域卫生信息平台实现了卫生系统垂直领域的信息共享，使更多的医务工作者可以接触到患者的个人健康信息；患者将病历信息上传至在线医疗服务平台做疾病咨询，问诊自查；患者将个人健康医疗数据上传至移动医疗 APP 用于分析数据；或患者通过移动可穿戴设备监测健康时所产生的健康数据、医患之间的在线沟通产生的数据等，这些平台在为患者提供医疗健康服务的同时，也沉淀了患者的个人健康医疗信息。而数据巨大商业利润的吸引无疑会导致个人健康信息的非法披露和交易。接触患者信息的主体多元化，意味着利益相关者的增加，无疑加大了个人信息泄露的风险。

4. 数据身份还原能力更强

健康医疗数据的激增以及来源多样性为大数据技术挖掘创造了条件，通过实现对个人身份的重新标识，让个人健康医疗信息保护面临更大的挑战。大数据对多源数据进行融合使得传统的匿名化和模糊化技术存在很大的局限性，单一的数据源通常对实体简单描述，但通过大数据技术对多个数据源进行融合之后，可以得到更加丰富的个人描述信息，进而识别出不同的实体。有文献指出，在基因大数据中，虽然对基因工程中 10 万个自愿者的邮政编码、出生日期与性别进行了匿名化操作，然而通过把基因序列数据与公共选民信息融合后，却重新甄别出 84%-87%自愿者的身份。所以对于复杂的大数据，即使利用匿名或者模糊化技术将个人敏感信息保护起来，但是当拥有其他公共的或者隐私的数据源时，可以利用链接攻击对匿名之后的数据源进行攻击，极有可能重新识别匿名后的个人敏感信息，这样造成个人隐私泄露[15]。

(三) 个人健康医疗信息保护的意义突显

在大数据背景下，曾经一度被归入隐私的个人信息逐渐体现出了独立的价值和内涵，近半个世纪以来有关个人信息保护的立法已然成为最为瞩目的立法运动之一。近年来，随着互联网时代的发展，运用大数据推动经济发展、完善社会治理、提升政府服务和监管能力正成为世界各国政策制定的趋势。

我国政府也认识到大数据的重要作用以及其对经济社会发展的巨大推动作用，从而积极推动相关行业大数据政策的制定和实施。健康医疗行业作为促进人的全面发展的基础性行业，其数据化和信息化的程度直接关系到人民的健康质量和生活水平，因此从中央政府到地方各省都在积极制定政策，鼓励和推动健康医疗大数据的发展和完善。

2015 年 8 月 31 日，国务院印发《促进大数据发展行动纲要的通知》（“《纲要》”）明确指出“数据已成为国家基础性战略资源”。作为《纲要》在健康医疗领域的延伸和发展，国务院办公厅于 2016 年 6 月 21 日发布《关于促进和规范健康医疗大数据应用发展的指导意见》（以下简称“《指导意见》”）。《指导意见》进一步指出“**健康医疗大数据是国家重要的基础性战略资源**”，并且指明了重点任务和重大工程。

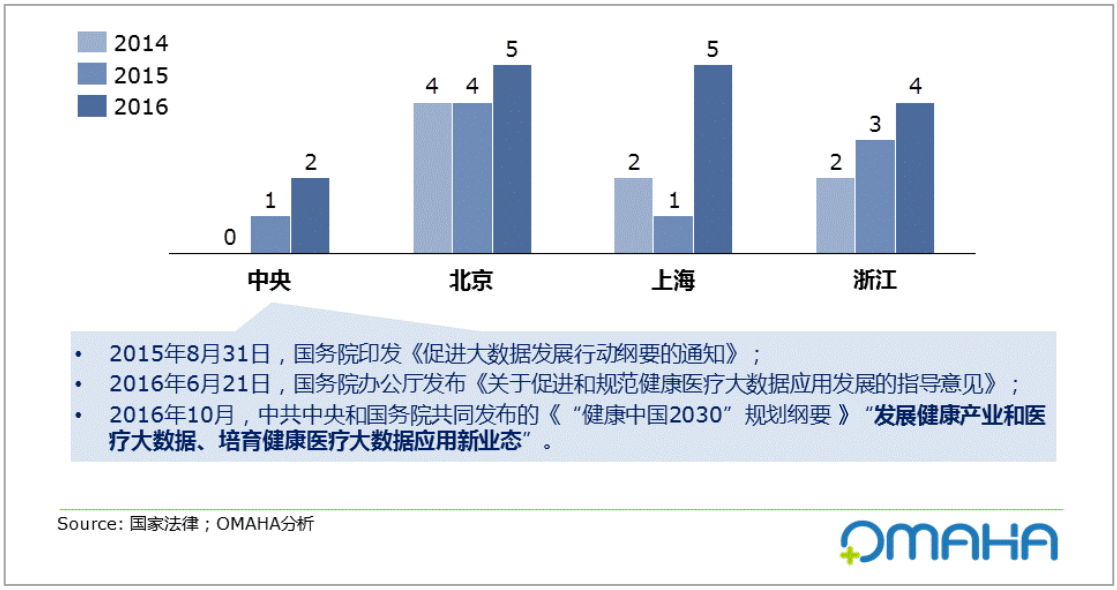
同时，强调“大力推动政府健康医疗信息系统和公众健康医疗数据互联融合、开放共享，消除信息孤岛，积极营造促进健康医疗大数据安全规范、创新应用的发展环境，通过‘互联网 + 健康医疗’探索服务新模式、培育发展新业态，努力建设人民满意的医疗卫生事业，为打造健康中国、全面建成小康社会和实现中华民族伟大复兴的中国梦提供有力支撑。”

作为《指导意见》在各地的落实和发展，截止 2016 年底，共有湖北省、云南省、四川省、河北省和重庆市等 5 个省市相继出台健康医疗大数据的配套实施意见。2016 年 10 月，

国家卫生计生委确定**福建省、江苏省及福州、厦门、南京、常州**为第一批健康医疗大数据试点省市，启动第一批健康医疗大数据中心与产业园建设国家试点工程。

2016 年 10 月，中共中央和国务院更是共同发布的《“健康中国 2030”规划纲要》。其中，“第二十三章 推动健康科技创新”和“第二十四章 建设健康信息化服务体系”专章对健康医疗相关的大数据服务提出要求，并且强调要构建国家医学科技创新体系、完善人口健康信息服务体系建设和推进健康医疗大数据应用。附录对国家和各自出台的健康医疗数据相关政策进行了详细列举，图 1 展示了 2014 年来北京、上海、浙江和国家出台相关政策的每年数据。

图 1：国家和主要省份发布的关于健康医疗数据的政策文件数量



与此相对应，计算机与互联网技术的飞速发展，从 web 2.0 到新媒体再到大数据，对信息收集、储存、处理、传播的愈发高效便捷，在提高生活便捷度、加快交易进程的同时，也大大增加了个人隐私被泄露或者被他人利用的风险。在当今这个去中心化、开放、共享的大数据时代，信息的流动呈几何增长的趋势。生活中无处不在的摄像头、智能手环等可穿戴医疗设备、内嵌于每个人智能电子设备上的定位系统、云存储上海量的数据信息等等，通过这些大数据技术手段与工具可以了解一个人的一举一动。

因此，就个人医疗健康信息以及以此为基础形成的健康医疗大数据，一方面其有效利用得以增进普罗大众之社会福祉，另一方面这些信息和数据频受侵害的风险也在不断地加大，无论从哪一个角度来讲，个人健康信息保护的议题都将是一个绕不开的话题。

二、 个人健康医疗信息的定义及其权利界定

(一) 个人信息的定义

工业和信息化部于 2013 年颁布的**《信息安全技术公共及商用服务信息系统个人信息保护指南》**对“个人信息”的定义为：可为信息系统所处理、与特定自然人相关、能够单独或通过与其他信息结合**识别该特定自然人**的计算机数据。个人信息可以分为个人敏感信息和个人一般信息。

- 个人敏感信息：指一旦遭到泄露或修改，会对标识的个人信息主体造成不良影响的个人信息。各行业个人敏感信息的具体内容根据接受服务的个人信息主体意愿和各自业务特点确定。可以包括身份证号码、手机号码、种族、政治观点、宗教信仰、基因、指纹等。
- 个人一般信息：除个人敏感信息以外的个人信息都为个人一般信息。

2013 年**《电信和互联网用户个人信息保护规定》**则从电信和互联网行业角度对“用户个人信息”进行了定义，即指电信业务经营者和互联网信息服务提供者在提供服务的过程中收集的用户姓名、出生日期、身份证件号码、住址、电话号码、账号和密码等能够单独或者与其他信息结合**识别用户**的信息以及用户使用服务的时间、地点等信息。

于 2016 年 11 月最新颁布的**《网络安全法》**[16]，应该说就“个人信息”确定了目前为止相对完备的一个概念，规定“个人信息是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”。且“任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。”

(二) 一对概念：“个人信息”和“隐私”

个人信息与隐私非常容易混淆，实质上两者有区别也有联系。

“个人信息”是指与一个身份已经被识别或者身份可以被识别的自然人相关的任何信息，包括个人姓名、住址、出生日期、身份证号码、医疗记录、人事记录、照片等单独或与其他信息对照可以识别特定的个人的信息。个人信息注重的是身份识别性，即只要求此种信息与个人人格、个人身份有一定的联系，无论是直接指向个人，还是在信息组合之后指向个人，都可以认为其具有身份识别性。从法律上看，凡是与个人身份有关联的信息，都可以看作是个人信息[17]。个人信息通常需要记载下来，或者以数字化的形式表现出来。而**“隐私”**主要是一种私密性的信息或私人活动，如个人身体状况、家庭状况、婚姻状况等，凡是个人**不愿意公开披露且不涉及公共利益的部分**都可以成为个人隐私。“隐私”是指私人生活安宁不受他人非法干扰，私人信息保密不受他人非法搜集、刺探和公开。隐私不限于信息的形态，它还可以以个人活动、个人私生活等方式体现，且并不需要记载下来。根据个人信息和隐私的定义，两者存在如下表 1 的区别。

表 1：个人信息和隐私的区别

	个人信息	隐私
属性	本质属性是“**识别性**”：通过个人信息能够将这个人“识别出来”。	重点在于不愿为外人所知的**“私密性”**，隐私主要是一种私密性的信息或私人活动。凡是个人**不愿意公开披露**且不涉及公共利益的部分都可以成为个人隐私。
权利内容	对个人信息的**支配和自主决定。**包括个人对信息被收集、利用等的**知情权**，以及自己利用或者授权他人利用的**决定权**等内容。即便对于可以公开且必须公开的个人信息，个人应当也有一定的控制权。例如，权利人有权知晓在多大程度上公开、向谁公开该信息以及他人会基于何种目的利用信息等。	隐私权主要包括维护个人的私生活安宁、个人私密**不被公开。**
违反	未经许可而**收集和利用**个人信息。	非法的**披露和骚扰。**

由于个人信息和隐私都体现了个人对其私人生活的自主决定，并且许多未公开的个人信息本身就属于隐私的范畴，因而隐私权与个人信息权时常被混为一谈。其实两者属于两个不同的范畴，二者的主要区别如表 2。

表 2：隐私权和个人信息权的区别

区别	个人信息权	隐私权
财产价值	集**人格利益与财产利益**于一体，既包括了精神价值，也包括财产价值。	是精神性的**人格权**，财产价值并非十分突出，主要体现的是人格利益。
行事形式	**主动性**，权利人除了被动防御第三人的侵害之外，还可以进行积极利用，如许可他人收集、处理自己的信息并获取相应报酬，或主动要求修改或删除有误信息。	呈现消极、**防御性**，在该权利遭受侵害之前个人无法积极主动地行使权利，只能在遭受侵害的情况下请求他人排除妨害、赔偿损失等。
损害的可逆性	可以被反复利用，损害通常具有**可恢复性。**	一旦被披露就不再是隐私，损害后果一般**不可逆。**
具体内容	对个人信息的支配和自主决定，包括个人对信息被收集、利用等的知情权，以及自己利用或者授权他人利用的决定权等，即便对于可以公开或必须公开的个人信息也享有一定的控制权。	维护个人的私生活安宁、个人私密不被公开、个人私生活自主决定等。
内容形态	以固定化的信息方式表现，通常需要记载或者以数字化的形式表现。	不限于信息的形态，可以以个人活动、个人私生活等方式体现，无需载体记载。

因此，隐私注重信息的“私密性”，个人信息注重“识别性”。两者之间的关系是：

- **个人信息可向隐私转化**，当个人不愿意公开披露个人信息时，该个人信息则转化成隐私信息。
- **个人信息的范畴容易确定**，即凡具标识个人的信息就为个人信息，而隐私的范畴则根据个人主观意志的改变而改变。同一个信息如果路人甲不愿意对外公开，那它就是路人甲的隐私，如果路人乙愿意向他人公开披露，则这些信息失去隐私权的保护，不属于隐私的范畴。

(三) 个人健康医疗信息的定义

《信息安全技术公共及商用服务信息系统个人信息保护指南》适用于电信、金融、医疗等领域，因此，个人健康医疗信息属于个人信息的一个分支，具备个人信息的一般属性。那么，什么是个人健康医疗信息呢，包括哪些内容?

据 2010 年卫生部印发《病历书写基本规范》规定：“病历是指医务人员在医疗活动过程中形成的文字、符号、图表、影像、切片等资料的总和，包括门（急）诊病历和住院病历。”

据 2014 年《人口健康信息管理办法（试行）》规定：“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[18]。”可见，人口健康信息指在医疗卫生计生服务机构可产生的信息，不包括院外产生的数据，如智能可穿戴设备产生的数据，范围较局限。

2016 年 6 月 24 日，国务院发布《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》，虽然该文件并未对健康医疗数据做出明确的定义，但正在鼓励“探索推进可穿戴设备、智能健康电子产品、健康医疗移动应用等产生的数据资源规范接入人口健康信息平台”，逐步开始推动非医疗卫生计生服务机构产生的数据与人口健康信息进行整合。

由此看出，随着 IT 和互联网的发展，个人的健康医疗信息的涉及范围在不断外延，从院内逐渐拓宽到院外患者个人产生的数据。在本白皮书中，我们统一采用“**个人健康医疗信息**”一词表达，并将其定义为：**能够识别出个人身份的所有健康医疗相关信息，包括各级各类医疗卫生计生服务机构产生的人口健康信息，和可穿戴设备、智能健康电子产品、健康医疗移动应用、网络在线平台等产生的个人健康医疗相关的信息。**

三、 国外对个人健康医疗信息的保护

(一) 美国

1. 主要法律法规的建设历程

随着医疗健康服务提供方的不断多元化，信息技术的不断发展，美国法律对个人健康医疗信息的保护经过的多次的调整和补充完善，最终形成了现有的法律体系（如图 2）。

1973 年，美国政府咨询委员会制定了《公平信息实施规范》（Code of Fair Information Practice），由公开、知情、二次使用、纠错和安全等 5 项基本原则组成。

1974 年，美国国会通过《隐私权法》（The Privacy Act），并于 1979 年将其编入《美国法典》，成为保护公民隐私权和知情权的基本法律。该法就政府机构对个人信息的采集、使用、公开和保密问题做出了详细规定，以规范政府处理个人信息的行为，平衡公共利益与个人隐私权之间的矛盾。这为后来的个人健康医疗信息隐私权保护奠定了基础。

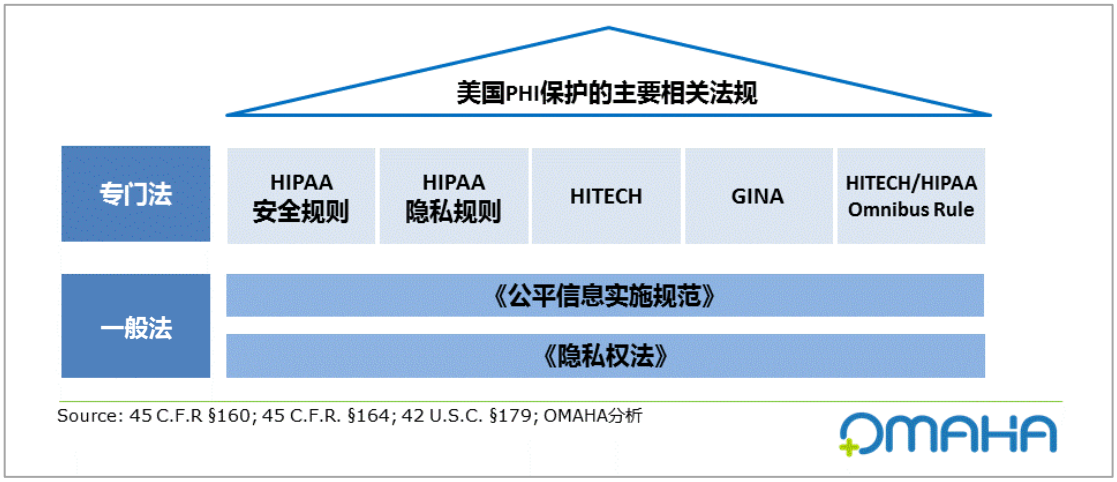
1996 年，美国国会颁布《美国健康保险携带与责任法》（Health Insurance Portability and Accountability Act，HIPAA），其最初目的是通过保护患者健康信息以帮助患者在更换工作时可以不受歧视的获得连续的健康保险。2003 年 4 月，HIPAA 隐私规则（Privacy Rule）和安全规则（Security Rule）生效。HIPAA 隐私规则对“受保护的健康信息”（Protected Health Information，PHI）和“适用主体”（Covered Entity，CE）进行了定义，确立了 PHI 接入、披露和使用的授权机制。HIPAA 安全规则为电子健康信息管理确定了具体安全措施。

2008 年《遗传信息无歧视法案》（Genetic Information Nondiscrimination Act，GINA）生效，对 HIPAA 条款进行补充，旨在保护个人不受基因信息带来的医疗保险或者受雇的歧视，确定了基因信息也是健康信息的组成部分。

2009 年，《经济与临床健康信息技术法案》（Health Information Technology for Economic and Clinical Health，HITECH）对 HIPAA 在隐私规则、安全规则和实施规则等部分做了修订，增加了新的保护条款；增加详细规定以确保患者自身对于个人健康医疗信息的获得权，支配权和使用权。

2010 年 7 月 HIPAA/HITECH Act Omnibus Rule 颁布并于 2013 年 3 月生效，从此“相关商业伙伴”（Business Associate，BA）被要求与 CE 遵守相同的法律准则，BA 成为 HIPPA 管辖范围内的法律实体。Omnibus Rule 大大增强了法律对 BA 的监管力度，减轻了 CE 对于 BA 的监管负担。

图 2：美国个人健康医疗信息保护的主要相关法规



2. HIPAA 及相关法案的一些重要概念

自 1996 年发布以来，将近 20 年的不断修订（2003 年、2009 年、2013 年），包括 HITECH 和 GINA 的相继出台，HIPAA 及其补充法案已经形成了一套系统、完整、详细且与时俱进的医疗健康信息领域的专门法。HIPAA 在全美范围内已执行多年，对保护个人健康医疗信息权益和促进美国健康医疗大数据的应用产生了不可磨灭的影响。**美国对于个人健康医疗信息保护，主要从个人隐私权的角度体现。**纵观全球，HIPAA 及其补充法案可以说是目前在个人医疗健康信息保护的专门领域最具影响力的一系列法案。

HIPAA 对约束范围内各类实体的定义、具体的隐私保护机制和安全措施都进行了详细规定，非常具有借鉴意义。

1) 受保护的健康信息（Protected Health Information，PHI）

HIPAA 提出“受保护的健康信息”（Protected Health Information，PHI），其定义为由**适用主体**或其**商业伙伴**持有或传输的以口头、书面和电子等任何形式或媒体存在的**可识别的个人健康信息**。

在法律层面对个人健康信息进行定义是对其进行保护的必要基础。值得注意的是，对于不能够识别个人的健康信息和不是由适用主体和其商业伙伴持有的健康信息，HIPAA、HITECH 和 GINA 对其并无约束力。

2) 可识别的个人健康信息（Individually Identifiable Health Information）

可识别的个人健康信息是健康信息的一个子集，指的是个人过去，目前和未来的生理和心理健康状况、医疗护理状况及与医疗护理相关的支付信息，并且这些信息包含了法律规定的能够识别出个人的 18 项身份识别信息（详见 4.2“脱敏机制”）中至少一项。

3) 适用主体（Covered Entity，CE）

定义中的适用主体（Covered Entity，CE）指的是三种受到 HIPAA 约束的法律实体，分别是医疗健康服务提供方、保险提供方和数据清洗公司，如图 3 所示其具体范畴。

图 3 ：HIPAA 约束范围内的三大 CE

医疗健康服务提供方（Health Care Provider）

- 医生
- 诊所
- 养老院
- 医学检验检查实验室
- 药店（实体/线上）

医疗健康保险提供方（Health Plan）

- 商业医疗保险公司
- 社会保险部门
- 健康管理机构（Health Management Organization，HMO）
- 公司保险计划

医疗健康数据清洗公司（Health Care Clearinghouse）

- 包括所有从其他机构得到数据后将非标准化医疗健康数据转化成标准化数据（比如标准电子格式或者数据形式）的公司。

4) 商业伙伴（Business Associate，BA）

在 HITECH Omnibus rule 生效之前，HIPAA 隐私条例仅仅对 CE 有约束力，然而随着医疗

服务需求增多以及医疗信息化的发展，绝大部分的医疗机构和保险公司都无法完全独立的完成所有的业务，而需要借助第三方机构或个人，越来越多的第三方机构通过 CE 获得了患者 PHI。为了加强对 PHI 的保护，美国法律将 BA 加入了管辖范围。法律条文中对 BA 提供的服务进行了举例，其中包括：

- 职能服务：健康数据分析、处理和管理；保险申诉处理和管理；质量管理；医保报销等；
- 其他服务：法务；审计；会计；咨询；数据采集；行政管理；认证和投资等。

常见的 BA 类型有：

- 为医疗机构提供个人健康档案（Personal Health Record，PHR）服务的机构或企业；
- 为医疗机构提供数据存储或数据分析服务的机构或者企业；
- 为医疗机构提供报销和收费服务的企业或机构；
- 为社会医疗保险或商业医疗保险机构提供处理索赔服务的企业或机构；
- 提供电子健康数据交换服务的机构（Health Information Organization，HIO）等。

3. 法律基本原则：HIPAA 隐私和安全规则

2003 年生效的 HIPAA 隐私和安全规则是个人健康信息保护的基础条例，适用于所有受 HIPAA 约束的 CE 和 BA。美国对个人健康信息的保护体现为对个人隐私权的保护，但美国的隐私概念与中国和欧盟的隐私概念都有明显的差别，属于“大隐私”类型：

- **美国法律赋予个人关于 PHI 的隐私权内容远远超过其他国家对隐私权的保护范畴；**
- **隐私权具体内容与欧盟数据保护的相关法律中体现的个人信息权非常相似。**

1) HIPAA 隐私规则

CE 对于任何非治疗、报销及医疗运营目的而使用和披露 PHI 时必须取得个人的书面授权（除为公共卫生控制，公众利益的使用以外）。患者的 PHI 信息指包含了 18 项可识别个人信息中任意一项的健康信息。对于 PHI 的脱敏过程本身就是使用 PHI，同样需要患者授权。

隐私规则的核心原则是对 PHI 的使用和披露需要满足**“最少必要”（minimum necessary）**。CE 必须保证披露 PHI 信息量和使用形式仅需满足患者授权使用目的的最低要求，能不披露尽量不披露，能不使用尽量不使用。

2) HIPAA 安全规则

HIPAA 安全规则包括对 ePHI（electronic Protected Health Information）的管理保护、实体保护和技术保护三方面，CE 和 BA 都必须按照安全规则规定对 PHI 进行保护。安全措施分为必选措施和自选措施，具体措施在法律条款中均有列出。

4. 关键业务场景的法规解析

随着产业和技术的发展，相关 BA 的加入增加了 PHI 管理的难度和复杂性，为此，HIPAA 对 BA 和 CE 之间的关系及权责做出了详细法律规定。

总体原则上，HIPAA 允许 CE 向 BA 披露 PHI，但两方之间的关系是服务和被服务，代表和被代表的关系。BA 必须提供书面承诺书（Satisfactory Assurance）并和 CE 签订相关商业伙

伴合同（Business Associate Contract）表示会遵守 HIPAA 隐私和安全规则，并只会为了满足 CE 的需求和目的而使用 PHI，不会将 PHI 用于任何自身的目的。与此同时，CE 和 BA 每次对 PHI 的披露和使用都必须满足 HIPAA 隐私条例的基本原则：**个人授权和最少必要原则。**

对于更加具体的涉及不同 BA 类型的业务场景，美国卫生和公共服务部（U.S. Department of Health & Human Services，HHS）及其下属的国家 HIT 协调办公室（The Office of the National Coordinator for Health Information Technology，ONC）作出了详细的法律解读和管理建议[19]：

1) HIT 机构或企业

HHS 将 HIT（Health Information Technology）定义为所有涉及**健康信息在电子环境中交换的技术**，而将所有涉及监督和管理健康信息的电子交换过程的企业或机构称为（Health Information Organization，HIO），HIO 也是最为常见的 BA 类型之一。常见的 HIO 包括区域健康信息组织（Regional Health Information Organization，RHIO），RHIO 通常负责在一定地理区域内的电子健康信息的互换，以提高医疗质量、安全和有效性。RHIO 的利益相关方通常包括：

- 提供医疗服务的机构
- 提供医疗保险报销的企业或者政府部门
- 与医疗质量提高相关的研究人员和机构
- 公共卫生部门
- 医疗服务的消费者

RHIO 提供的服务包括但不限于：

- 在各个法律实体的数据库中为个人匹配健康医疗信息
- 为 HIO 网络中的所有法律实体提供电子健康信息交换的基础条件
- 管理个人对于其健康信息的隐私保护偏好

HIO 在监督和管理电子健康信息交换的过程中需要遵守以下原则：

- **可更正原则**：应当提供个人及时的途径参与讨论其个人可识别健康信息的准确性和完整性，并能够更正错误信息，或记录下讨论的内容和结论；
- **公开和透明原则：**与个人或其可识别个人健康信息相关的政策，流程以及技术应当完全公开透明；
- **保护原则**：可识别个人健康信息应当被给予合理的管理，技术和实体的保护以确保其保密性，完整性和可及性，并预防未授权或不正当的接入，使用或披露；
- **限制采集、使用和披露原则**：可识别个人健康信息应当只因完成特定目的的必要而被采集、使用或披露，并且绝不应当受到不恰当的歧视；
- **责任性原则：**以上提到原则应当通过恰当的监管和相应的报告手段被确保执行。

相关业务流程

以 RHIO 为例，实现区域内的电子健康信息互换需要通过以下步骤：

- 首先持有 PHI 的所有医疗或保险机构等 CE 需要获得个人授权后才能向 RHIO 披露患者 PHI 信息；

- RHIO 需要与网络内的 CE 进一步签订相关商业伙伴合同以明确 RHIO 所需要提供的服务。同时 HIPAA 允许 RHIO 与其网络内所有 CE 签订一份多边协议以简化流程。

2) PHR 服务提供商

HHS 通将个人健康档案 PHR 理解为一份个人健康信息的电子记录。患者可以查看这些健康信息，亲自控制谁能够获得这些信息，并能借此参与自己的健康管理，而有相当部分的医疗机构（属于 CE）通过第三方机构（属于 BA）向患者开放 PHR。

根据 HIPAA 规定，BA 在向个人提供 PHR 服务时必须确保个人能够：获得个人 PHR；添加个人信息进入 PHR，并能够更新和编辑自己输入的信息；允许其他人查看自己的 PHR，比如伴侣、家庭成员或者其他的医生。

相关业务流程

医疗机构通过第三方机构向患者开放 PHR，必须通过以下步骤[1]：

- 首先医疗机构需要根据法律规定确定 PHR 开放的最小数据集；
- 医疗机构需要获得患者授权后才能向商业机构披露患者 PHI 信息；
- 医疗机构必须和商业机构进一步签订相关商业伙伴合同，明确商业机构的权责（只能以开放 PHR 为目的对 PHI 进行最低限度的使用）。

3) 研究机构

第三方研究机构的加入可以加强对健康数据的分析，提高对电子健康信息的利用，同时 CE 和 BA 仍然需要遵守 HIPAA 规定对 PHI 进行披露和使用。

相关业务流程

根据总体原则，若某 CE 希望通过第三方机构来完成一项数据分析，需要经过以下步骤：

- CE 需要确定此次分析的研究目标；
- 根据研究目标确定需要向第三方机构披露的最小数据集；
- CE 需要获得患者授权才能向研究机构披露 PHI；
- 医疗机构必须和商业机构进一步签订相关商业伙伴合同，明确研究机构的权责（只能就此次研究目标对数据进行分析）。

4) 云计算服务提供方

云计算（Cloud Computing）解决方案已被医疗机构广泛使用，云服务提供方（Cloud Services Provider，CSP）可提供的服务涵盖很广，包括从简单存储电子病历信息到开发新软件的平台。CE 和 BA 也对是否能够在保护 ePHI 的同时利用云计算的巨大优势十分关注。

值得注意的是，根据 HIPAA 规定，哪怕 CSP 仅仅储存加密后的 ePHI 且没有密钥，CSP 仍然属于 BA 或 BA 的分包方（Subcontractor），必须签订相关商业伙伴合同并遵守 HIPAA 的相关法规。

[1] 注：如果 PHR 服务提供方是一个完全独立的机构，不与任何医疗机构相连接，不从医疗机构获取数据，完全由患者个人负责上传 PHR，则不受到 HIPAA 的约束。

相关业务流程

如果 CE 或者 BA 需要 CSP 提供服务需要经过以下步骤：

- CE 或者 BA 需要获得患者授权后才能向 CSP 披露患者 PHI 信息；
- CE 需要和 CSPs 进一步签订相关商业伙伴合同，明确商业机构的权责；如果 CSP 属于 BA 的分包方，则需要与 BA 签订相关商业伙伴合同。

5. 关键管理和技术要求的法规解析

1) 信息的所有权

尽管在美国法律中确定了个人对 PHI 的控制权、决定权和支配权等权力，但在美国法律中并未对由 CE 产生、持有和保管的个人健康医疗信息的所有权作出明确的规定，对于数据的所有权是属于医疗机构还是患者本人，在美国国内也一直存在较大的争议。但通常与 BA 签订的合同中，CE 可以明确表明 **BA 对于 PHI 没有所有权。**

2) 相关商业伙伴合同

CE 本身对 PHI 的使用和披露已受到 HIPAA 的严格约束，在此基础上，商业伙伴合同（Business Associate Contract）可以让 CE 进一步约束商业机构对于 PHI 的使用和披露，此合同通常包括商业机构承诺书的内容，并受到 HIPAA 保护，即 BA 必须承担 HIPAA 规定的所有义务，但不享有除合同中 CE 批准以外的对于 PHI 的任何权利[20]。

商业伙伴合同通常包括以下内容：

- 基本概念的定义；
- BA 的义务：
  - 允许 BA 对 PHI 使用和披露的范围（尽量详细）；
  - 禁止 BA 对 PHI 使用和披露的范围（尽量详细）；
  - 对于提供患者隐私安全必要技术保障的承诺；
  - BA 必须承诺报告任何不恰当的接入、用和披露；
  - 明确商业机构对数据没有所有权；
- 合同终止的时间（具体时间点，或者约定可以导致合同终止的违约情形）。

3) 授权机制

CE 对于任何非治疗、报销及医疗运营必须而使用和披露 PHI 时必须取得个人的书面授权（Authorization）。值得注意的是，如果授权内容发生任何变化或授权已过期，对同一位患者的 PHI 披露仍然需要再次授权。

- 授权主体：CE 请求 PHI 对应的个人进行授权；
- 授权形式：书面授权（线下纸质签名或线上电子签名）；
- 授权内容：以下内容必须明确清晰告知患者：
  - 信息接收方名称；
  - 披露的具体信息内容（e.g. 性别、药品名称、某次手术名称、某次检验检查等详细信息）；
  - 披露目的（e.g. 为了让患者查看、下载和传输病历信息）；

- 不进行授权会带来的后果（e.g. 无法查看自己的病历信息）；
- 授权的过期时间（e.g. 完成此次病历下载后、此次研究结束后等）。

4) PHI 交易

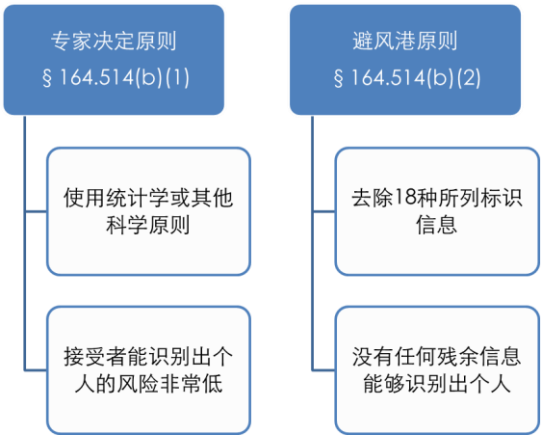
HIPAA 明确禁止**未经患者本人授权**的任何形式的 PHI 交易或利用 PHI 进行市场推广的行为。对于市场推广的行为，法律也进行了明确定义："为协助其他实体鼓励接受方购买或使用某产品或服务，CE 向其披露 PHI，并换得了直接或间接的经济补偿。"同时法律也明确禁止医疗机构出售在其机构治疗的患者名单。

5) 脱敏机制

如果 PHI 信息依据有关标准和要求经脱敏（De-identifying）操作转变为去识别化 PHI，对其使用和发布则不再受 HIPAA 隐私规则的限制。但值得注意的是，HIPAA 规定对 PHI 的脱敏本身就是对 PHI 的使用，这也就意味着，对于接触到 PHI 的 BA 来说，没有与 CE 达成协议的情况下不能将 PHI 进行脱敏并进一步使用。

对于去识别化受保护的健康信息流程，HIPAA 法案给出了两套细则：专家决定原则和避风港原则，如图 4 所示。

图 4 ： HIPAA 隐私规则中的脱敏方法



a) 专家决定原则

个人健康数据持有机构可以通过专家评审的方法决定哪些信息是需要去除的，专家必须在决定个人可识别信息领域拥有相当的统计学和科学知识阅历，专家需根据个人健康数据接收机构无法通过获得信息识别出个人的原则决定去除哪部分信息的，并且记录下作出决定的方法、过程和结果。

b) 避风港原则

以下 18 种可能识别出个人，或者其亲属、雇主、家庭成员的信息需要去除：

- 姓名；
- 小于省级的地址，包括街道，城市，地区和三位以后的邮编；
- 除年份以外与个人相关的日期，包括（生日、进院日、出院日、死亡日期、超过 89 岁的年龄）；

- 电话号码；
- 车辆登记号码、车牌号码；
- 医疗器械标识号和序列号；
- 传真号码；
- 电子邮件；
- URL；
- 社保号码；
- IP 地址；
- 病历编号；
- 指纹等生物标记信息；
- 医疗保险号码；
- 正面全脸照片；
- 银行账户号码；
- 证件号码（身份证、驾照等）；
- 任何其他可用于识别的编码或特征。

6) 脱敏后的身份还原/数据再识别

随着大数据技术的发展，对于脱敏后个人信息的再识别（Re-identification）成为可能。HIPAA 规定任何被再次识别出个人的数据不再是脱敏数据，而重新成为了 PHI，持有者需根据 HIPAA 规定对其进行使用和保管。

6. 超出 HIPAA 保护范畴的个人健康医疗信息

根据法律的规定，超出法律保护范畴的个人健康信息可分为两类：脱敏后的个人健康信息和非 CE 或其 BA 所持有的个人健康信息，如图 5 所示。

1) 脱敏后的个人健康信息

尽管美国医疗行业内仍然对脱敏后数据的买卖和使用存在不同的意见和争议，但 2011 年美国联邦最高法院在 Sorrell vs. IMS Health 一案中的判决表明，美国的立法和司法对脱敏后的健康医疗数据的运用保留了一些灵活的余地。该案件涉及为了医药公司的市场推广目的，药房出售脱敏后患者的处方药数据，法院最终判决药房并没有违反法律。虽然案件具有一定的特殊性和复杂性，但在一定程度上确立了出售脱敏后个人健康数据并不违反法律规定的司法基调。

2) 非 CE 或其 BA 所产生或持有的个人健康信息

由于各类网络社交平台的兴起，大量由个人有意或无意分享的个人健康信息充斥在网络社交平台上，已有公司通过收集和分析社交平台上的个人健康信息，根据所得结果进行定向的药品推广。此类问题也引起了很多学者的思考和讨论，但目前非 CE 或其 BA 所产生或持有的个人健康信息还不属于 HIPAA 保护的范畴。具体举例如下：

- 患者产生的数据（Patient-Generated Health Data）

- 由个人上传到 PHRs 服务提供商的个人健康信息，此类的 PHRs 服务提供商有 Google Health， Microsoft Myhealth Vault；
- 个人在社交网站和 APP 上分享的个人健康信息；
- 各类移动端软件产生的个人生物体征（步数、心率等），包括患者自测的指标。

- 独立的非 CE 基因检测机构直接从患者采取得到的数据
  - 此类的机构有在线基因检查公司 23andMe、Ancestry.com 等。目前此类机构受到美国 FDA 管理和行业内的自我监察。

图 5 ： HIPAA 的保护范围界定

(二) 欧盟

1. 欧盟的立法体制

欧盟法律体系既不同于国内法体系，也不是传统的国际法体系。欧盟法律和各成员国间既具有直接适用的一元关系，也具有非单一等级的二元关系。总体而言，欧盟法立法层面主要包括欧盟基础条约（包括《欧盟联盟条约》与《欧洲联盟运行条约》），以及根据基础条约制定的**条例（Regulation）、指令（Directive）和决定（Decision）**。

- **欧盟条例**对于成员国和成员国内个人和机构具有直接适用性，无需经过各成员国以国内立法形式体现而可以直接于国内实施；
- **欧盟指令**则是针对各个成员国发布，由成员国自行选择实施方式，一般给予成员国一定期限将其根据各国情况转化为国内法；
- **欧盟决定**则是针对特定对象的约束性法律文件，特定对象可以是特定或全部成员国、特定机构或个人或特定产品，虽然效力上对特定对象具有直接适用性，但适用范围不具有普遍性。

目前，欧盟对于个人健康医疗信息保护，主要从个人数据和网络信息安全角度体现。包括 1995 年制定的《关于个人数据处理中个人权利保护及促进数据自由流通的指令》（“1995 年《指令》”，将被 GDPR 取代），和 2016 年通过的《一般数据保护条例》（General Data Protection Regulation，GDPR）、《网络与信息系统安全指令》（Directive on Security of Network and Information Systems，NIS）和《欧盟—美国隐私盾》（EU-U.S. Privacy Shield，《隐私盾协议》）等。

除上述欧盟信息保护一般立法外，基于欧盟法，以及在欧盟法尚未覆盖的特别领域，欧盟各成员国可以制定关于个人信息保护或者个人健康医疗信息保护的国内立法。例如：德国于 2015 年通过了一项旨在加快医疗保健行业数字化进程的《电子医疗法》，由于电子医疗将涉及病患敏感信息，该法案要求电子病历的医疗应用应按照参保人意愿开展，除法律允许的必要基本数据和医疗人员读取急救信息外，相关数据的提供、存储、修改和传递应由参保人自主或授权操作。另外，德国的《联邦个人数据保护法》和《社会法典第五卷》含有大量个人数据保护的规定，GDPR 通过后，目前德国卫生部正在同联邦数据保护部门合作打造更安全的防护网络。

2016 年英国脱离欧盟，将不会适用 GDPR 等欧盟法，即使在脱欧之前英国也明确表示英国将保留数据保护方面立法的自主权。2012 年，英国通过了《医疗和社会保障法》（Health and Social Care Act），明确赋予英国国家医疗服务体系数字服务部（NHS Digital）[2]权力，直接从全英国的家庭医生处收集其掌握的健康医疗数据，再由 NHS Digital 负责对外的数据开放利用[21]。英国脱欧后，将不再适用包括《隐私盾协议》在内的欧盟规则，英国将如何修改、补充相关立法，以弥补英国和欧盟、美国等之间的数据转移保护规则的空白，仍有待观察。

鉴于 GDPR 将于 2018 年实施，而《网络与信息系统安全指令》给予了成员国 21 个月的期限将其转化为国内法，欧盟各国目前实施的国内法可能在未来两年内有较大修改，以符合欧盟法要求更好地保护欧盟数据和信息安全，相应地对个人健康医疗信息采取更严格的保护措施。

2. 《一般数据保护条例》（General Data Protection Regulation，GDPR）

1) GDPR 出台的背景

大数据时代的挑战。1995 年欧洲议会通过《关于个人数据处理中个人权利保护及促进数据自由流通的指令》，规定了个人数据保护的最低标准和目标，并对个人数据的跨国流通进行了严格限制。然而当时信息技术的发展尚处于初级阶段，个人数据的搜集和整理在广度和深度上都十分有限。而今互联网等技术的数据量呈几何级爆炸式增长，1995 年《指令》已难以有力应对个人数据被非法窃取、利用和监控以及跨境数据的安全流动等难题。

统一法律规则的需要。由于 1995 年《指令》的立法层级不高，而欧盟各成员国根据本国文化传统和技术水准制定了不同的数据保护执行标准和制度，导致个人数据在不同国家享有的保护水平不同。如此不仅弱化了数据保护的整体效果，还使得成员国间的数据流动效率较低，加重了企业的负担。

在这样的背景下，欧盟 GDPR 于 2016 年 5 月 24 日生效，并将于 2018 年 5 月 25 日实施。新出台的 GDPR 取代了 1995 年《指令》。而且，不同于 1995 年《指令》，GDPR 将直接适用于每个欧盟成员国和个人或机构，更有利于成员国之间的数据流动和保护标准的统一，并对欧盟的数据保护产生更深远的影响。

[2] 注：原为医疗和社会保健信息中心（Health and Social Care Information Centre，HSCIC），2016 年 8 月 1 日改名为 NHS Digital。

2)　GDPR 赋予数据主体的权利

GDPR 将个人数据定义为“任何与已识别或可识别自然人（“数据主体”）相关的信息”，包括能够直接或间接揭示自然人的种族、政治倾向、宗教和信仰、商业资格、个人健康等的数据，并明确提及基因数据和生物数据作为个人健康数据加以保护。除非在特定例外条件下，包括数据主体的同意，或者数据主体已经将上述信息公开；为了建立、履行或者保护合法的诉求必须处理上述敏感信息；为了公共利益的需要，或者与公共利益相关的归档、科学、历史或者统计目之外，不得对个人数据擅自处理。

另外，GDPR 第九条规定成员国未来可以针对基因、生物识别以及健康数据的保护进行进一步规定。基于 GDPR 对个人数据的定义，数据主体享有如下权利：

a)　删除权（被遗忘权）

- 当用户依法撤回同意或数据控制者不再有合法理由继续处理数据时，用户有权要求删除数据；
- 如果数据控制者在前述情况中将所涉个人数据进行了公开传播，则应该采取所有合理的方式通知处理此数据的其他数据控制者删除关于数据主体要求删除的个人数据的链接、复制。

但应注意，若所涉数据的处理为行使言论自由权、履行有关公共利益的法律义务、特定情况下的公共利益以及起诉或答辩所必需，则删除权的行使将受限制。

b)　知情权

个人数据从数据主体处取得时应告知：

- 数据控制者的身份和联系方式及其指定代表的信息（如有适用）；
- 数据保护专员（Data Protection Officer，DPO）的相关信息（如适用）；
- 数据处理的目的和法律依据。若为数据控制者或第三方的合法利益之目的确有需要使用个人数据，则应告知该等合法权益；
- 数据的接收者或数据接收者的类型（如适用）；
- 如果数据传输到第三国或国际组织，则需要告知用户该第三国是否通过欧盟的充分性决定，若未通过则需要告知数据控制者采取了何种保障措施。

个人数据非从数据主体处取得时应告知：

- 个人数据的保留周期以及确定该等周期的理由；
- 从数据控制者处要求获取、改正或删除个人数据、限制或反对数据处理的权利，以及数据可携带权；
- 若数据处理是基于数据主体的同意，则应告知撤回同意的权益，并且撤回不得影响先前的数据处理中用户的合法利益；
- 向监管机构投诉的权利；
- 其个人数据的来源和类型；
- 个人数据从数据主体处取得时应告知的所有内容。

c)　访问权

数据控制者应当提供相应的访问流程，若数据主体以电子形式提请访问，则数据提供的

方式也应当采取电子形式。控制者不能就此收费（除非数据主体的请求明显过量）。

d) 反对权

- 数据主体有权拒绝数据控制者基于公共利益或数据控制者或第三方的合法利益处理个人数据，除非存在强制性法律基础比数据主体的利益、权利和自由更重要；
- 数据主体有权拒绝为直接市场营销之目的对其个人数据的处理。

e) 限制处理权

- 在数据主体对个人数据的准确性提出异议时，在数据控制者验证数据准确性期间有权限制该等数据的处理；
- 非法处理的情形下，数据主体有权要求限制数据的使用而非删除该等数据。

f) 数据可携带权

数据主体可以无障碍地将其个人数据从一个信息服务提供商转移至另一个信息服务提供商，该等信息的形式应有序、常用且可机读。

3. 《网络与信息安全指令》（Directive on Security of Network and Information Systems，NIS）

欧盟议会于 2016 年 7 月 6 日正式通过《网络与信息系统安全指令》，旨在于欧盟范围内实现统一高效的网络与信息系统安全保护，并加强国际合作。NIS 中，网络与信息系统安全，是指网络与信息系统有能力抵抗针对经由这些网络与信息系统存储、传输、处理、提供的信息或者相关服务的可用性、真实性、完整性或者保密性等采取的破坏措施。NIS 要求成员国制定网络安全国家战略，加强成员国间合作与国际合作，要求在网络安全技术研发方面加大资金投入与支持力度，提升打击跨国网络犯罪的力度，同时要求基础服务运营者、数字服务提供者履行网络风险管理、网络安全事故应对与通知等义务以提升网络与信息系统安全。

NIS 于 2016 年 8 月生效，成员国须于指令生效 21 个月之内将其转化为国内法，并在 27 个月内完成对指令涉及的公共服务重点领域企业的梳理[22]。

1) NIS 指令出台的背景

随着信息技术的疾速发展，网络空间已成为与物理世界平行的人类活动场所，但由于其兼备开放性和匿名性特征，成了一个易攻难守之地。欧盟委员会清晰地意识到了网络在人类生活中的广泛存在性，支撑着经济、医疗、能源、交通等各大系统正常高效的运作；同时犯罪分子、恐怖分子、自然灾害或不经意间的错误都可能造成网络安全事故，扰乱或严重破坏与人们日常生活息息相关的设施与服务。面对新兴科技的发展——电子支付、云服务、机器互动等，欧盟意识到其网络需要更高的安全度，为防止事故、恶性事件或不当使用的发生，2016 年 7 月发布了欧盟层面首个网络安全领域的规则。

欧盟 NIS 地位相当于欧盟的首部网络安全法。**NIS 的适用主体是关键服务运营商和数字服务提供商，欧盟各成员国可根据主体定义的指导原则，自主确定具体的范围。**如同我国新近颁布的《网络安全法》提出“关键信息基础设施”概念一样，NIS 指令也启用了“关键服务运营商”的概念，并且明确地将健康产业（医疗设施，包括医院以及私人诊所）纳入了“关键服务运营商”的范畴。同时，数字服务提供商的纳入是此部指令的重大突破，扩大了管理范围，充分适应数字时代的发展。

2) NIS 对关键服务运营商（Operators of Essential Services，OES）的定义

a) 关键服务运营商的认定标准

- 提供的服务对关键的社会或经济活动是必需的；
- 服务的提供依赖于网络和信息系统；
- 若出现安全事故将会对该等重要服务的提供造成破坏性影响。

b) NIS 指令涵盖的关键服务运营商所在行业范围

- 能源：电力、石油、天然气；
- 交通：航空、铁路、水路、陆路；
- 银行：征信机构；
- 金融市场基础设施：交易所、主要交易方；
- 健康产业（医疗设施，包括医院以及私人诊所）；
- 水：饮用水供应与分布；
- 数字基础设施：互联网交换中心、域名系统服务提供商、顶级域名注册机构。

c) 关键服务运营商的义务

- 报告义务：向国家监管机关报告严重的网络安全事件；
- 风险预防：采取与风险相对应的技术和组织措施；
- 安全确保：采取安全措施以确保网络与信息系统具备能够应对风险的安全度；
- 事故处理：采取安全措施以预防事故对服务提供所使用的信息技术系统产生的影响，并将该等影响最小化。

3) NIS 对数字服务提供商（Digital Service Providers，DSP）的定义

a) NIS 指令涵盖的数字服务提供商范围

- 在线交易场所：商家能够在交易场所开设店铺，在线提供产品和服务；
- 云计算机服务；
- 搜索引擎。

b) 数字服务提供商的义务

- 报告义务：向相关部门报告较大的网络安全事件；
- 风险预防：采取与风险相对应的技术和组织措施；
- 安全确保：采取安全措施以确保网络与信息系统具备能够应对风险的安全度；
- 事故处理：采取安全措施以预防事故对服务提供所使用的信息技术系统产生的影响，并将该等影响最小化；
- 其他措施：采取其他相关安全措施，包括维护本公司系统和设备的安全性、持续经营管理、监管、审计、测试以及遵守国际标准。

4. 《欧盟—美国隐私盾协议》（EU-U.S. Privacy Shield）

欧美“安全港”协议被欧盟法院判决无效的背景下，经过欧盟和美国的多次谈判，欧盟委员会于 2016 年 7 月 12 日通过了《隐私盾协议》以取代安全港协议。《隐私盾协议》强化了欧盟的数据主权，将更有利于欧盟公民利用 GDPR 维权。

1) 《隐私盾协议》出台的背景

美欧对个人数据保护程度不同。美国偏向更灵活保护的策略，通过企业自律机制并配合政府执法，来实现保护隐私权的目的；欧盟却倾向于通过严厉的立法，对个人数据跨境流动进行保护。欧盟早在 1995 年《指令》出台时就通过第 25 条确立了“充分性保护”标准， 并要求美国企业在开展业务时遵守要求。而通过《安全港协议》，美国商务部建设了一个公共目录，遵守相关义务并加入目录的企业成为“安全港”成员，从而满足欧盟政策门槛拥有数据转移资格。但《安全港协议》一直被视为两种保护体系妥协的产物，存在诸多问题。例如，根据协议规定，“安全港”目录企业可以不经个人授权转移数据，因此欧盟专家质疑该协议损害欧盟数据主权和公民隐私；而只有被美国联邦贸易委员会和交通部监管的机构才能加入“安全港”目录，而其他机构无法加入目录而不能在欧美之间进行数据传输将影响其业务开展。 另外 2013 年的“棱镜门事件”也让欧盟产生了对《安全港协议》是否能充分保护欧盟数据主权和数据市场的质疑[23]。

欧美《安全港协议》被废止。2013 年，奥地利律师 Schrems 向 Facebook 欧洲总部所在地爱尔兰当局提出申诉，控告 Facebook 非法追踪用户数据，参与美国情报机构的监控计划。欧盟法院于 2015 年 10 月 6 日判决 2000 年签署的保障跨大西洋数据流动的欧美《安全港协议》制度无效。本是便利企业进行数据跨境流动的“桥梁”被废除，美欧之间只能通过企业一对一的合同方式处理跨境数据流动，效率低下且成本提高。

因此，作为欧美双方寻求跨境数据流动的制度性保障措施，2016 年 7 月，《隐私盾协议》应运而生。

2) 《隐私盾协议》主要内容

a) 增强数据主体权利

- 详细规定七项原则：知情原则、选择原则、转移原则、安全原则、数据完整原则、访问原则、执行原则；
- 突出数据主体个人数据保护的救济机制：（1）向企业进行投诉，企业应当在 45 日内给予答复；（2）向本国的数据保护机构投诉，该机构可与美商务部、联邦贸易委员会合作进行调查和处理；（3）求助于免费的替代性纠纷解决机制，名单内企业都必须加入这一机制；（4）求助于隐私保护专家组进行仲裁，其做出的裁决具有约束性。

b) 落实数据控制者的义务

- 企业通过自主认证“自愿加入”后，必须公示其入盾承诺及相应的隐私政策；
- 企业在入盾后还需完成定期自证审查，并接受联邦贸易委员会、运输部等部门的调查与监督；
- 当企业未完成定期验证时，商务部将撤销其入盾的资格，企业也将归还或删除相应的数据。

c) 权力约束

- 美国政府应避免大规模无差别的监控；
- 美国将在美国国务院内设立一个独立于国家安全部门之外的监察专员岗位，负责处理来自欧盟公民就个人数据问题的投诉与问询，并监督国家情报部门的数据访问；
- 美国国家情报部门专家及欧盟数据保护机构将共同负责年度审查。

(三) 美国和欧盟对个人健康医疗信息保护的共性

虽然美国和欧盟法律在立法体制和执法方式等等诸多方面存在很大差异，但美国法律赋予个人关于 PHI 的隐私权具体内容与欧盟法律中体现的个人信息权非常相似：都强调个人对于个人健康医疗信息拥有**支配权、决定权和控制权**。具体可以包括但不限于以下方面：

- **个人有权获得自己的个人健康医疗信息**
  - HITECH 中明确规定患者有获得 PHR 的权利；
  - GDPR 指出数据主体可以访问个人数据；
- **个人有权修改错误的个人健康医疗信息**
  - HITECH 中明确规定患者有权修改 PHR 中个人输入的信息；
  - GDPR 指出数据主体对个人数据具有反对权；
- **个人有权清晰知晓了解个人健康医疗信息被披露和使用的内容、目的及主体**
  - HIPPA 隐私规则中明确授权书中必须包括以上内容并清晰告知患者；
  - GDPR 指出数据主体对个人数据具有知情权；
- **个人有权撤回对个人健康医疗信息的披露或使用授权**
  - HIPPA 隐私规则中明确授权书中告知患者拥有撤回授权的权力；
  - GDPR 指出数据主体对个人数据具有被遗忘权；
- **个人有权不受阻碍的向另一个医疗机构传输个人健康医疗信息**
  - HITECH 中明确规定个人有权下载和传输个人 PHR；
  - GDPR 指出数据主体对个人数据具有数据可携带权。

四、 我国对个人健康医疗信息的保护

有关个人信息或隐私的保护，我国不仅在法律法规体系建设方面已经完成了基本的框架搭建，在健康医疗领域的相关立法和政策布局工作也取得了很多进展，包括国家和地方层面出台了一系列的政策和指导意见。而 2016 年 11 月《网络安全法》的颁布，以及目前仍处于立法进程中的《民法总则》将个人信息保护纳入权利保护框架的动议，更是将我国的个人信息保护的立法制度建设提高到了一个新的高度。

(一) 关于个人信息保护的相关立法

1. 一般性个人信息保护的法律框架

按照目前的法律法规体系，个人信息保护主要依赖政府执法即公权保护，个人只有在隐私信息受到侵害的情况下方能寻求私权救济。

从公权保护维度，关于个人信息保护的规定散见于法律法规、部门规章、司法解释中，且仅针对适用于特定场景并基于个人在特定场景下所具有的特定身份。如，在互联网场景下，个人基于网络用户的身份，所涉及的个人信息受《网络安全法》及相关规定保护；在市场经济活动中，个人基于消费者的身份，所涉及的个人信息受《消费者权益保护法》及相关规定保护；在劳动用工场景下，劳动者的个人资料受《就业服务与就业管理规定》及相关规定保护。此外，对于某些特定行业（如金融、医疗）中产生的个人敏感信息，行业主管部门还出台针对性的保护措施。但因我国尚未出台《个人信息保护法》，个人信息其实并不能得到全面、系统的保护。

从私权保护维度，2009 年《侵权责任法》首次明确隐私权属于民事权益的一种，同时还进一步明确规定医疗机构及其医务人员对患者资料的保密责任。但如本文第二部分所述，个人信息和隐私在属性和权利内容方面均存在较大差别，因此仅从隐私权角度很难对所有个人信息施以全方位的充分保护，容易出现保护真空。虽然 2014 年《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》将个人隐私外的其他个人信息也列入保护范围，但保护场景局限于网络环境且以当事人受损害为前提，能达到得保护效果有限。

我们梳理总结了目前关于一般性个人信息保护的规范性法律文件及相关条文，按照效力层级罗列如下：

1) 法律法规

- **《网络安全法》**: 2016 年 11 月 7 日正式颁布，首次综合系统地规定了个人信息的保护，提高了个人对其信息的管控程度，引入删除权和更正制度；明确了个人信息保护相关主体的法律责任，（1）网络运营商收集、使用个人信息必须符合合法、正当、必要的原则，目的明确的原则、知情同意的原则等，应遵守对收集信息的安全保密原则、公民信息境内存放原则、泄露报告制度等，（2）要求关键信息基础设施运营者遵守公民信息境内存放原则，确需向境外提供的信息，应进行相应的安全评估，（3）要求网络产品、服务的提供者收集个人信息时应向用户明示并取得同意，还要遵守相关公民个人信息保护的规定；明确了对侵害公民个人信息行为的惩处措施。（第 22、37、40-50 条）
- **《宪法》:** 保护公民的通信自由和通信秘密，除因国家安全或者追查刑事犯罪的需要，由公安机关或者检察机关依照法律规定的程序对通信进行检查外，任何组织或者个人不得以任何理由侵犯公民的通信自由和通信秘密。（第 40 条）

- **《刑法》**：《刑法修正案（七）》增加了出售、非法提供公民个人信息罪、非法获取公民个人信息罪，《刑法修正案（九）》进一步拓宽了该罪的适用范围，不再局限于国家机关或者金融、电信、交通、教育、医疗等单位的工作人员。（第 253 条）
- **《侵权责任法》**：明确隐私权属于民事权益的一种，规定医疗机构及其医务人员应当对患者的隐私保密，泄露患者隐私或者未经患者同意公开其病历资料，造成患者损害的，应当承担侵权责任；医疗机构及其医务人员应当按照规定填写并妥善保管住院志、医嘱单、检验报告、手术及麻醉记录、病理资料、护理记录、医疗费用等病历资料。（第 2、61、62 条）
- **《刑事诉讼法》**：规定了在证据的收集和使用中、技术侦查过程中，对涉及个人隐私的数据应当保密；涉及个人隐私的案件不公开审理。（第 52、150、183 条）
- **《民事诉讼法》**：涉及隐私的证据应当保密，不在公开开庭时出示；涉及个人隐私的案件不公开审理；公众可以查阅发生法律效力的判决书、裁定书，但涉及个人隐私的内容除外。（第 68、134、156 条）
- **《消费者权益保护法》**：消费者在购买、使用商品和接受服务时，享有个人信息依法得到保护的权利；经营者收集、使用消费者个人信息，应遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经消费者同意；收集、使用消费者个人信息，应当公开其收集、使用规则，不得违反法律、法规的规定和双方的约定收集、使用信息；对收集的消费者个人信息必须严格保密，不得泄露、出售或者非法向他人提供；经营者应当采取技术措施和其他必要措施，确保信息安全，防止消费者个人信息泄露、丢失，在发生或者可能发生信息泄露、丢失的情况时，应当立即采取补救措施。（第 14、29、50 条）

2)　国务院规范性文件及全国人大常委会的相关决定

- **《全国人大常委会关于加强网络信息保护的决定》**：明确规定国家保护能够识别公民个人身份和涉及公民个人隐私的电子信息，并要求遵从国际惯例规定了多项个人信息保护和利用的基本原则。
- **《全国人民代表大会常务委员会关于维护互联网安全的决定》**：非法截获、篡改、删除他人电子邮件或者其他数据资料，侵犯公民通信自由和通信秘密的，可构成犯罪。（第 4 条）
- **《国务院关于促进市场公平竞争维护市场正常秩序的若干意见》**：要求在保护涉及公共安全、商业秘密和个人隐私等信息的基础上，依法公开在行政管理中掌握的信用信息；依法规范信用服务市场，推动建立个人信息和隐私保护的法律制度，加强对信用服务机构和人员的监督管理。（第 16 段）

3)　部门规章及规范性文件

- **《信息安全技术公共及商用服务信息系统个人信息保护指南》**：定义个人信息保护中涉及的术语，明确个人信息管理者在使用信息系统对个人信息进行处理中的八项原则：目的明确原则、最少够用原则、公开告知原则、个人同意原则、质量保证原则、安全保障原则、诚信履行原则和责任明确原则；细化收集、加工、转移、删除四个主要环节的信息保护规范。
- **《电信和互联网用户个人信息保护规定》**：定义了用户个人信息，信息收集和使用规范、安全保障措施作出了详细的规定，包括：未经用户同意，电信业务经营者、互联网信息

服务提供者不得收集、使用用户个人信息；对在提供服务过程中收集、使用的用户个人信息应当严格保密，不得泄露、篡改或者毁损，不得出售或者非法向他人提供；电信业务经营者、互联网信息服务提供者保管的用户个人信息发生或者可能发生泄露、毁损、丢失的，应当立即采取补救措施等。

- **《即时通信工具公众信息服务发展管理暂行规定》**：即时通信工具服务提供者应当落实安全管理责任，保护用户信息及公民个人隐私。（第 5 条）
- **《规范互联网信息服务市场秩序若干规定》**：收集个人信息需经用户同意，不得将用户个人信息提供给他人；应当明确告知用户收集和处理用户个人信息的方式、内容和用途，不得收集其提供服务所必需以外的信息，不得将用户个人信息用于其提供服务之外的目的。（第 11、12 条）
- **《就业服务与就业管理规定》**：用人单位应当对劳动者的个人资料予以保密。公开劳动者的个人资料信息和使用劳动者的技术、智力成果，须经劳动者本人书面同意。（第 13 条）

4) 司法解释

- 《最高人民法院关于确定民事侵权精神损害赔偿责任若干问题的解释》：人民法院应当受理违反社会公共利益、社会公德侵害他人隐私或者其他人格利益，受害人以侵权为由向人民法院提起的赔偿精神损害诉讼请求。（第 1 条）
- 《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》：网络用户或者网络服务提供者利用网络公开自然人基因信息、病历资料、健康检查资料、犯罪记录、家庭住址、私人活动等个人隐私和其他个人信息，造成他人损害，被侵权人请求其承担侵权责任的，人民法院应予支持。（第 12 条）

2. 有关个人健康医疗信息保护的专门立法

目前健康医疗领域关于个人信息保护的法律法规比较零散，不够系统、全面且主要针对传统的健康医疗场景从而存在一定程度滞后性，表现为（1）在适用主体方面，虽然《人口健康信息管理办法（试行）》、《执业医师法》、《护士条例》分别规定了医疗机构、医生和护士对于患者个人信息保护的职责，但目前健康医疗领域的法规体系无法全面囊括健康医疗领域的其他参与方，如移动医疗服务提供方、健康医疗数据存储和平台运营方等；（2）在保护客体方面，受保护信息范围基本还是针对院内信息。如《医疗机构病历管理规定》：明确规定医疗机构及其医务人员应当严格保护患者隐私，禁止以非医疗、教学、研究目的泄露患者的病历资料，同时还规定了病历的保管保存以及病历的借阅与复制事宜；《人口健康信息管理办法（试行）》对人口健康信息的定义虽然宽泛，但该类信息仍局限于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信息，从而也就间接限制了信息范围；（3） 未能清楚界定健康医疗信息的权属问题，限制患者获取个人健康医疗信息并掣肘健康医疗大数据的发展。

个人健康医疗信息保护方面的规范性法律文件及相关条文总结、罗列如下：

- **《医疗机构病历管理规定》：**明确规定医疗机构及其医务人员应当严格保护患者隐私，禁止以非医疗、教学、研究目的泄露患者的病历资料。同时还规定了病历的保管保存以及病历的借阅与复制事宜，包括：医疗机构应当严格病历管理，任何人不得随意涂改病历，严禁伪造、隐匿、销毁、抢夺、窃取病历；住院病历由医疗机构负责保管，患者出

院后，住院病历由病案管理部门或者专（兼）职人员统一保存、管理，患者不得带走住院病历；除特定人员、部门外，其他任何机构和个人不得擅自查阅患者病历；患者本人或者其委托代理人、死亡患者法定继承人或者其代理人有权申请复制或者查阅病历资料，受理复制病历资料的申请时应审核申请材料等。（第 6、10-23、28-30 条）

- **《电子病历系统功能规范（试行）》**：要求患者隐私保护功能包含：（1）必须的功能（对电子病历设置保密等级的功能，对操作人员的权限实行分级管理，用户根据权限访问相应保密等级的电子病历资料；授权用户访问电子病历时，自动隐藏保密等级高于用户权限的电子病历资料。当医务人员因工作需要查看非直接相关患者的电子病历资料时，警示使用者要依照规定使用患者电子病历资料）；（2）推荐的功能（提供对电子病历进行患者匿名化处理的功能，以便在必要情况下保护患者健康情况等隐私）。（第 11 条）
- **《人类遗传资源采集、收集、买卖、出口、出境审批行政许可服务指南》**：由科技部批准之后方可：将人类遗传资源传输至境外；与外方或外商投资企业合作采集人类遗传资源；采集特定区域或重要遗传家系的遗传资源。
- **《医疗事故处理条例》**：患者有权复印或者复制其门诊病历、住院志等病历材料；但对于以医疗事故为由，寻衅滋事、抢夺病历资料，扰乱医疗机构正常医疗秩序和医疗事故技术鉴定工作的，可给予刑事或治安管理处罚。（第 8-10、59 条）
- **《执业医师法》**：医师在执业活动中应保护患者隐私，泄露患者隐私造成严重后果的将受到行政处罚甚至刑事处罚。（第 22、37 条）
- **《护士条例》**：护士应当尊重、关心、爱护患者，保护患者的隐私，泄露患者隐私的将受到行政处罚，包括吊销执业证书。（第 18 条）
- **《涉及人的生物医学研究伦理审查办法》**：涉及人的生物医学研究应当遵守保护隐私原则（切实保护受试者的隐私，如实将受试者个人信息的储存、使用及保密措施情况告知受试者，未经授权不得将受试者个人信息向第三方透露）；伦理审查委员会审查的内容包括是否有对受试者个人信息及相关资料的保密措施。（第 18、20、46 条）
- **《人口健康信息管理办法（试行）》**：（1）规定人口健康信息定义，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；（2）在职责划分上，规定县级以上人民政府卫生计生行政部门（含中医药行政部门）是人口健康信息主管部门；国家卫生计生委负责制订全国人口健康信息发展规划和管理规范，统筹指导全国人口健康信息管理工作；县级以上地方人民政府卫生计生行政部门负责推进、指导、监督本行政区域人口健康信息管理工作；各级各类医疗卫生计生服务机构（含中医药服务机构，下同）负责人口健康信息的采集、利用、管理、安全和隐私保护，是人口健康信息管理中的责任单位；（3）规定了责任单位采集、利用、管理人口健康信息时应遵循的相关规则。

3. 立法趋势

2003 年国务院信息管理办公室曾委托中国社会科学院法学研究所个人数据保护法研究课题组起草《个人信息保护法》（专家建议稿），2005 年该专家建议稿提交，标志着我国第一部有关个人信息保护的法律《个人信息保护法》的立法程序正式启动。然而十余年过去，《个人信息保护法》依然尚未出台。目前虽仍有人大代表持续呼吁制定《个人信息保护法》，以满足保护个人信息安全、维护公民基本人权的需要，但随着《网络安全法》的颁布以及《民法总则》立法进程的推进，《个人信息保护法》在短期内似乎已不大可能纳入全国人大的立法议程。

即将于 2017 年 6 月 1 日实施的《网络安全法》首次在法律层面专门地、详细地规定了个人信息的保护。而《民法总则》（草案）则拟将个人信息权作为基本民事权利，明确予以法律保护。这些立法趋势无不表明个人信息权或者个人信息受保护的权利将被进一步确认，并受到更为明确、具体的保护。

(二) 司法实践解读

1. 刘春泉诉中国工商银行股份有限公司上海市分行侵权责任纠纷再审申请案，（2016）沪民申 2161 号，2016.12.1

再审申请人刘春泉在工行办理银行卡的领用合同中允许工行向其发送“与牡丹信用卡有关的信息”。之后工行向其发送商业信息，刘春泉认为其个人信息受保护的权利受到损害，提起诉讼。再审申请人刘春泉认为，损害不能显性化和具体量化不等于无损害，更不能因此判决不构成侵权。个人信息权受损本身就是不显性化的，对于这种难以确定具体损失的侵权行为我国法律早有规定。上海市高级人民法院认为，工行向其储户发送商业信息可以解释为领用合同中与牡丹信用卡有关的信息，未违反社会公共利益和社会公德，故尚不足以造成对个人信息受保护权利的损害。

2. 彭魏、李建标、陈金辉犯侵犯公民个人信息罪案，（2016）琼 9003 刑初 150 号，2016.7.28

海南省儋州市人民法院认定被告人违反国家有关规定，向他人出售、提供公民个人信息，侵犯公民的个人信息权，情节严重，已构成侵犯公民个人信息罪。

3. 王洁诉中国联通鸿盛精品手机城、界首市鸿盛手机经营部等买卖合同纠纷案，（2015）界民一初字第 00680 号，2015.8.11

原告主张被告在升级系统、检修手机的过程中，将其手机存储的原告个人信息和资料丢失，从而侵犯了其信息权和隐私权。对此，安徽省界首市人民法院称“原告王洁没有提供相应的证据，以证明被告泄露、出售或非法向他人提供了其个人信息或个人隐私，仅凭原告王洁的个人陈述，达不到证明被告侵犯其信息权、隐私权的目的”，可见界首市人民法院将（个人）信息权视为与隐私并行而非附属的概念，承认了（个人）信息权的独立地位。

4. 赵信强诉温州市仙人球文化传媒有限公司网络侵权责任纠纷案， (2015)温乐民初字第 159 号，2015.3.26

浙江省乐清市人民法院称“网络用户或者网络服务提供者利用网络公开自然人基本信息等个人隐私和其他个人信息，此类行为已然涉嫌侵权”，由此可见该院并未将个人信息完全归属于个人隐私的范畴。

小结：

司法实践中，部分法院并未将个人信息完全归属于个人隐私的范畴，甚至承认了个人信息的独立地位。《刑法》中的侵犯公民个人信息罪，同样从侧面印证了公民个人信息权，因为承认了公民个人信息权或者个人信息受保护的权利，才能存在侵犯公民个人信息的行为甚至犯罪。但是值得注意的是，鉴于目前生效的民事法律法规中并未直接将个人信息权作为独立权利予以保护，法院民事判决中个人信息（权）和隐私权的保护通常表现出一致性，一方面主张个人信息和隐私权被侵权的一方需要承担举证责任，另一方面在不涉及隐私权的个人信息侵权中，法院的判决则相对谨慎。

(三) 与欧美保护实践的对比分析

作为立法落地、政策推行和制度建设的参照样本，在隐私权和个人信息保护上我国对于欧美的经验和实践多有参考和借鉴。正如之前在欧美对比分析中所指出，基于商业传统、市场经济环境和规则理念培育的不同，**在隐私权和个人信息保护上，美国更强调商业机构的自律，并辅之以政府的执法；而欧盟则更倾向于通过严厉而完备的立法来实现保护的目的。**而从整体的立法体系而言，我国的民事法律制度构建基本沿袭了德法等欧洲大陆国家为主的大陆法系传统。因此，我国的立法和政策取向，更多地可以借鉴欧盟的实践，其中包括界定“关键信息基础设施”、设定个人信息保护的权利边界、完善权利救济手段以及整合政府的数据保护职能等。但美国作为网络技术和数据应用最为发达的国家，其诸多的行业实践和成功经验也对我国提供了相当丰富的学习标本。

回到医疗健康产业，我国在国家政策和行业实践层面，医疗健康大数据都发展得如火如荼。然而，即便已经取得了令人瞩目的成绩，我国现有的法律法规却仍不足以应对随之产生的对个人信息的各种侵害。对比美国和欧盟的相关立法，我国针对个人信息的法律规定上存在如下不足之处：

1. 个人信息权定位不明

至今为止尚无法律明确个人信息权是否系独立于隐私权、名誉权等现有权益之外的一项权利，法院判决中涉及侵犯个人信息的案例多将其归于隐私权或名誉权，单独承认（个人）信息权的案例十分有限。如此模糊的定位和不同的司法解读相当不利于个人信息的保护，尤其是未纳入隐私范畴内的其他个人信息，而权利被侵犯后也难以得到足够的救济。期待《民法总则》（草案）通过后能保留有关个人信息权的规定，明确其独立的法律地位。

2. 法律规定不成体系

如第一部分所列，我国对个人信息保护的规定散见于法律法规、部门规章、司法解释，法律体系上缺乏呼应。现有的针对互联网信息管理和个人信息保护的法律法规之间协同性差，不成体系，呈现“群龙无首”的局面。在缺乏统一立法的情况下，部分行业规定提及了对个人信息的保护，而尚未制定相关规定的行业则留下了制度空白。此外，虽然《网络安全法》在一定程度上弥补了立法的空白，但对于线下个人信息的保护仍缺乏统一的规制。

3. 法律条款内容空洞

目前我国的诸多法律法规对个人信息保护的条款均采取“对 xxx 在工作中获取的个人信息应予以保密”的表述，十分原则和笼统，缺乏细致、具体的操作规范，例如针对在获取/处理个人信息过程中应采取何种安全措施、对信息主体负有何种具体义务等，均付之阙如。而与美国 HIPPA（包括其隐私规则和安全规则）和欧盟 GDPR 长达数十页的详尽的规定相比，我国针对个人信息保护的法律条款未免显得过于单薄、空洞。

4. 处罚力度尚有不足

《刑法》对侵犯公民个人信息罪规定了刑事处罚，包括拘役/有期徒刑和罚金；《网络安全法》是目前为止对侵犯个人信息的罚则规定得最明晰的法规，包括警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。相比之下，GDPR

规定的罚金可谓巨额：对于侵权行为的罚金可达 1000 万欧元或全球年收入的 2%，不执行监管机关命令的罚金更是高达 2000 万欧元或全球年收入的 4%。

五、 对加强个人健康医疗信息保护的建议

(一) 对政府的立法建议

1. 制定《个人信息保护法》

建议政府尽快制定并出台《个人信息保护法》，作为个人信息保护的基本法律调整公私领域内的个人信息保护与利用之间的关系，保留《民法总则（草案）》中对个人信息权的单独规定，再通过《个人信息保护法》进一步巩固加强个人信息权有别于隐私权、名誉权、一般人格权的法律地位。由于目前在我国尚未形成充分的市场自律氛围，因此由国家统一立法加以规范尤为必要。申言之，我国急需通过立法位阶高的统一法律来规定适合我国国情的个人信息保护的基本原则、信息主体的权利、信息行业从业者和政府的义务、法律责任等，确立我国个人信息保护的门槛标准。《网络安全法》在一定程度上借鉴了欧盟 GDPR 的有关内容，但其规定仍然较为笼统，信息主体所享有的权利和数据收集、应用和处理者应承担的义务仍不够明晰。

同时，建议法律的规制和监管要和技术的发展同步，避免相关立法的滞后。例如在大数据技术快速发展的背景下，个人敏感信息脱敏后的再识别在技术方面越来越容易实现，因此，如何保证立法与技术的同步接轨，以及如何保证行业对法规的有效遵从等，将是个人信息保护领域的现代立法需要持续考虑和关注的命题。

2. 赋予信息主体更全面的权利

1) 知情权

尽管《网络安全法》在一定程度上明确了用户的知情权（网络产品、服务具有收集用户信息功能的应当向用户明示并取得同意）；《医疗机构病历管理规定》、《医疗事故处理条例》也明确了病人对其病历资料的知情权（可借阅、复制病历），但该等知情权的范围未免过于狭隘。相比之下，GDPR 规定的知情权的内容广泛很多，细分为数据从信息主体处直接取得和从信息主体外取得两种情形，需要告知的内容包括：数据控制者的身份和联系方式及其指定代表的信息、数据的接收者或数据接收者的类型、数据处理的目的和法律依据、个人数据的保留周期、从数据控制者处要求获取、改正或删除个人数据、限制或反对数据处理的权利、数据可携带权、向监管机构投诉的权利等。我国法律规定应进一步扩大个人知情权的范围，可以考虑各个行业切入，细致规定知情权的范围。

2) 删除权/被遗忘权

除知情权外还应当赋予个人删除权（被遗忘权）。2014 年 5 月，欧洲法院在 Google 诉西班牙数据保护局及冈萨雷斯中作出突破性判决，认定搜索引擎应负有对“不适当、不相关、过时的数据信息”的删除责任，否则侵犯公民在网络领域所享有的“被遗忘权”。自此之后，“被遗忘权”在全球范围内引起了广泛关注和热烈讨论，GDPR 也正式确定了删除权（被遗忘权），即当用户依法撤回同意或数据控制者不再有合法理由继续处理数据时，用户有权要求删除数据。如果数据控制者在前述情况中将所涉个人数据进行了公开传播，则应该采取所有合理的方式通知处理此数据的其他数据控制者删除相关链接、副本。

目前我国的相关规定有《网络安全法》第 43 条“个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正”；《全国人大关于加强网络信息保护的决定》第 8

条“公民发现泄露个人身份、散布个人隐私等侵害其合法权益的网络信息，或者受到商业性电子信息侵扰的，有权要求网络服务提供者删除有关信息或者采取其他必要措施予以制止”；《信息安全技术公共及商用服务信息系统个人信息保护指南》第 5.5.1 条“个人信息主体有正当理由要求删除其个人信息时，及时删除个人信息。删除个人信息可能会影响执法机构调查取证时，采取适当的存储和屏蔽措施”。也就是说，我国目前的规定只及于第一层数据控制者，倘若该等错误或侵权信息已被公开传播，公民还需逐一通知其他各网站、媒介予以删除，对公民而言无疑负担过重、可操作性低。相比之下，立法应该加重数据控制者的义务，在该等情形下要求其承担删除错误、侵权信息的义务。

3. 设立专门的数据保护机构

我国可借鉴欧盟设立专门的数据保护机构的做法，建立独立的个人信息保护管理机构，确保我国个人信息保护法的实施。欧盟的数据保护机构包括欧盟委员会、欧盟理事会、欧盟议会、第 29 条工作组、欧盟数据保护专员，以及成员国国内的数据保护机构。同时，在全球经济一体化背景下，该专门管理机构也有利于我国在个人信息跨国流通过程中更好地参与国际合作，维护我国国家信息主权和公民的信息利益。就我国目前的机构设置现状来看，可以考虑以现有的国家互联网信息办公室为平台，适当整合信息产业、工商管理等部门的部分职能，建构该专门管理机构，由其负责监督个人信息保护法的实施、展开个人信息保护执法调查、进行个人信息保护与利用研究等，并适时向立法机关提出立法意见和建议等。

4. 增加有效救济手段

目前我国法律提供的救济手段单一，重刑事和行政处罚，轻民事确权和归责，导致信息主体的财产及非财产损失往往得不到实质性的赔偿，并且救济手续繁琐耗时，缺乏灵活性。建议借鉴 GDPR 第 82 条的规定，即一项数据侵权行为若涉及多个数据控制者与处理者，则每一个控制者和处理者负有连带责任，若数据控制者和处理者可以证明自己不对该损失负责，则可以全部或部分免除责任，这种对连带责任与举证责任倒置规则的明确将使数据主体获得更为有效的救济。此外，欧美《隐私盾协议》给予数据主体的多重救济机制同样具有参考价值，包括：（1）向企业进行投诉，企业应当一定期限日内给予答复；（2）向国家数据保护机构投诉，该机构可进一步与有关国家机关合作（如工信部、信息办等）进行调查和处理；（3）求助于替代性纠纷解决机制；（4）求助于隐私保护专家组进行仲裁，其做出的裁决具有约束性。多元化的救济手段对信息主体和企业而言都更灵活，有益于个人信息纠纷的解决。

5. 明晰云计算、大数据的使用权限

随着大数据和云计算的普及，大量的个人数据收集和分析成为可能，政府和企业的决策越来越依赖大量的数据收集和分析。在这种情况下，数据挖掘、分析技术使数据被利用的可能性增加，数据被收集、使用的风险增大。《个人信息保护法》可以从立法上明晰个人隐私与公共信息涉及的不同范围界限，明晰公权力进入个人隐私、个人信息范围的界限，明晰可以开放和共享的信息范畴。

6. 规定智能终端个人信息保护

如今，我国的互联网已进入移动互联网时代。《个人信息保护法》应当对移动 APP 产业链上的相关主体提出针对性条文，明确移动 APP 开发者必须遵循的基本原则：提供易懂、易得的隐私政策；对数据的披露、收集和处理需取得用户明确的授权；告知用户修改、删除、拒绝等权利；在 APP 设计和实施各个阶段进行隐私设计确保安全。

7. 明确健康医疗大数据领域的外资准入条件

在目前的网络和数字技术的发展态势之下，任何一国都不可能只谋求在本国范围之内讨论大数据的应用和个人信息的保护问题。在我国，目前总体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，但在部分细分领域则存在一些细化的规定。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。

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。

(二) 对医疗机构的应用建议

1. 推行和应用信息交换标准，促进医疗信息的可携带性

如今的经济下，迁徙已成常态，因而确保医疗和医疗保险关系和待遇的可接续性已然成为一个与人们生活密不可分的问题。同时，生命的连续性要求医疗服务必须是连续的，而医疗信息的连续、完整是医疗服务安全、有效的保证。医疗大数据已与区域的人口和社会政策、疾病和健康情况、医药研发和医疗技术创新密切相关，最终必将对经济和社会发展带来巨大影响，因此当医疗信息的可携带性已成为个人医疗信息的必备条件之一，以便医疗机构之间以及医疗机构与其他机构（如保险公司）高效高质的数据交换。

而标准是实现医院信息平台互联互通、电子病历信息共享、电子医疗信息可携带的基础。当美国的医疗市场全面电子化之后，建立了全国性的信息标准，美国全境的医疗服务提供方均需依据全国性信息标准采集、上传和储存。电子信息标准化可以避免“信息孤岛”，当前我国医院间检查化验不能互认，其中一个原因就是因为标准不一致。如果能建立区域乃至于全国的医疗和医保数据管理标准，这将大大提高数据的质量和交换效率。2016 年 8 月，国家卫生计生委发布了《电子病历共享文档规范 第 1 部分：病历概要》等 57 项卫生行业标准，自 2017 年 2 月 1 日起生效，建立了一套适合我国、科学规范的电子病历共享文档规范，从而为卫生信息互联互通标准化成熟度测评提供数据标准支持。该标准是国家层面电子病历基本数据传输与交换标准，主要满足医院信息平台互联互通、电子病历信息共享，实现区域医疗卫生服务协同和数据共享。作为医疗服务主要提供者的医疗机构，在推行和应用数据标准上应当担负起首要的责任。

2. 与商业伙伴签订协议约定信息保护义务

HIPAA 规定了适用主体（主要包括医疗机构和医务人员）与商业伙伴之间应当签订协议，协议须包含的内容包括但不限于：（1）描述商业伙伴就受保护医疗信息经允许的用途；（2）规定商业伙伴不得为协议允许或要求以外的目的，或违反法律要求，使用或披露受保护医疗信息；（3）要求商业伙伴采取恰当的安全保护措施，以防受保护医疗信息的使用或披露与

协议约定相违背。若适用主体获悉商业伙伴发生重大违约或违法行为，则适用主体应采取合理措施弥补或终止该等违约、违法行为；若该等措施失败，则应终止与商业伙伴签订的协议或所做的安排。美国 HHS 还提供了商业伙伴协议模板供参考。我国医疗机构同样可以借鉴，达到严格管理商业伙伴的信息处理行为的目标。

(三) 对相关商业机构的合规建议

1. 规范健康医疗数据的采集活动

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，并通过隐私政策（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；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。

以可穿戴医疗设备为例，可穿戴医疗设备监测数据内容多且不易理解，监测时间长、综合性强，数据使用者更为广泛，知情同意告知难度大。因此，需要建立有针对性的知情同意规范，明确告知佩戴者采集的持续时间、数据内容等，保证个人信息的收集是建立在合理合法的基础之上，并有义务将数据使用目的和使用权限告知，并征得其本人同意。

虽然目前中国法下尚未明确规定公民对个人信息享有的权利，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。作为商业机构，在实践中可以考虑借鉴和学习合规标准较高的跨国企业的公司政策和行业规范。

2. 确保数据本地化存储及境外传输的合规

《网络安全法》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。

在目前强调网络空间主权的形势下，商业机构须尽量做到在中国本地化存储健康医疗大数据。在无法确定对外输出数据是否构成危害国家安全、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。

3. 加强集团公司内部管理

自上而下的立法保护模式在信息技术日新月异的今天已明显不足，在此背景下，自下而上的行业推动或许显得尤为难能可贵。建议我国商业机构可参照 GDPR 第 47 条规定，就公司集团或组织内部的跨境数据转移设置对本公司及相关人员有约束力的规则，包括但不限于：

- 可传输的数据类型；
- 对数据的处理形式与目的；

- 对内及对外的约束程度；
- 有限的数据存储周期；
- 对特殊/敏感数据的处理方式；
- 确保数据安全的相应措施；
- 投诉/申诉渠道。

4. 完善安全保护技术措施

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 年制定的《信息安全等级保护管理办法》、卫生部于 2011 年发布的《卫生行业信息安全等级保护工作的指导意见》以及最新的《网络安全法》都对信息系统的安全等级保护制度提出了明确的要求。

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，建议健康医疗大数据运营商参照卫生部在《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，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个人信息数据发生泄露、毁损或丢失的情况。在发生或者可能发生信息泄露、毁损或丢失的情况时，应当立即采取补救措施。

(四) 对个人的建议

对个人健康医疗信息的保护，不仅需要来自政府从立法角度对整个行业的监督和管理；医疗机构及相关商业机构自身的强化自律和相互监督，更需要公众整体提高个人健康医疗信息素养，增强自我保护意识和能力，在目前国内相关立法和执法尚不完善的情况下尤其重要。具体可体现为以下几方面：

1) 注意保护个人健康医疗信息，在信息泄露前就应做到防微杜渐，不随意透露个人健康医疗信息，不对未经认证的健康设备予以授权，仔细阅读授权书内容，从源头防止个人健康医疗信息被恶意利用；
2) 注意识别各种欺诈手段，防止个人健康医疗信息泄露或者被不当利用；
3) 了解、学习个人健康医疗信息方面得政策法规。当个人健康医疗信息遭受侵害时，应主动维权，如个人健康医疗信息被非法泄露时，主动报警或寻求专业法律人士的帮助，利用法律的力量维护自己的合法权益。

六、 结束语

OMAHA 倡导完善个人健康信息相关权益的保护机制，推进个人及各行各界对健康医疗大数据的有序利用，释放健康医疗数据的极大价值。为此，OMAHA 作为 NGO，可向有意愿推动个人健康信息相关权益的保护机制建立的医疗机构和商业机构提供以下支持，共同完成这一美好愿景：

- 进行国内外相关法律或行业标准调查和分析，向机构和企业提供相关的研究成果；
- 就具体的业务场景，建立相关的管理和法律咨询通道，帮助行业对数据的规范利用；
- 帮助个人进行与个人健康医疗信息保护相关的法律常识科普。

感谢您对健康医疗数据开放事业的支持！

OMAHA 团队：朱烨琳、周子琳、吴垚、胡红林
汉坤律师事务所团队：朱敏、张驰、孙冠绯

附录

表 3：我国中央及地方政府对推进健康大数据应用的政策举例

中央层面健康医疗大数据政策	• 2015 年 8 月 31 日，国务院印发《促进大数据发展行动纲要的通知》； • 2016 年 6 月 21 日，国务院办公厅发布《关于促进和规范健康医疗大数据应用发展的指导意见》； • 2016 年 10 月，中共中央和国务院共同发布的《“健康中国 2030”规划纲要》。
主要地方健康医疗大数据政策	**各地对中央《指导意见》具体落实文件：** • 2016 年 10 月 10 日，湖北省政府办公厅《关于促进和规范健康医疗大数据应用发展的实施意见》； • 2016 年 11 月 4 日，云南省政府办公厅《关于促进和规范健康医疗大数据应用发展的实施意见》； • 2016 年 11 月 3 日，云南省卫计委《关于印发云南省“互联网+健康医疗”行动计划（2016-2020 年）的通知》； • 2016 年 11 月 7 日，四川省卫计委、发改委和人保厅《关于加快推进互联网+医疗健康服务的指导意见》； • 2016 年 11 月 7 日，河北省政府办公厅《关于促进和规范健康医疗大数据应用发展的实施意见》； • 2016 年 12 月 23 日，重庆市政府办公厅印发《重庆市健康医疗大数据应用发展行动方案（2016—2020 年）的通知》。
	北京市健康医疗大数据政策： • 关于继续深化医药卫生体制改革的若干意见（2014.09.29，市政府）； • 关于促进健康服务业发展的实施意见（2014.09.23，市政府）； • 关于加快推进中关村生物医药医疗器械及相关产业发展的若干意见（2015.02.16，市政府办公厅）； • 关于积极推进“互联网+”行动的实施意见（2016.01.09，市政府）； • 关于印发《北京市大数据和云计算发展行动计划（2016—2020 年）》的通知（2016.08.03，市政府）； • 关于印发《北京市“十三五”时期信息化发展规划》的通知（2016.12.01，市政府）； • 关于印发落实深化医药卫生体制改革 2014 年重点工作安排任务分工方案的通知（2014.09.10，市卫计委）； • 关于印发《首都卫生和计划生育领域知识产权管理工作指南（试行）》的通知（2014.12.03，市卫计委）； • 关于印发 2015 年人口健康信息化工作要点的通知（2015.04.30，市卫计委）； • 关于市委社会事业与社会治理体制改革专项小组改革实施规划（2014-2020 年）分工方案（2015.06.23，市卫计委）； • 关于印发《2015 年大型医院巡查及改善医疗服务行动计划工作方案及有关实施细则》的通知（2015.09.15，市卫计委）； • 关于加强北京市康复医疗服务体系建设的指导意见（2016.06.14，市卫计委、市发改委、市教委、市经信委、市民政局、市财政局、市人保局、市金融局、市残联）； • 关于开展健康体检电子信息采集工作的通知（2016.11.15，市卫计委）。

表 4（续）

主要地方健康医疗大数据政策	**上海市健康医疗大数据政策：** • 关于促进本市生活性服务业发展的若干意见（2014.09.19，市政府）； • 关于印发《上海市推进“互联网+”行动实施意见》的通知（2016.02.01，市政府）； • 关于印发《上海市深化医药卫生体制综合改革试点方案（2016-2020 年）》的通知（2016.05.19，市政府）； • 上海市科技创新“十三五”规划（2016.08.05，市政府）； • 关于印发《上海市大数据发展实施意见》的通知（2016.09.15，市政府）； • 关于印发《上海市推进智慧城市建设“十三五”规划》的通知（2016.11.11，市政府）； • 上海工业及生产性服务业指导目录和布局指南（2014 年版）（2014.04.16，市经信委）； • 上海关于印发《上海市进一步改善医疗服务行动计划实施方案》的通知（2015.04.03，市卫计委）。
	浙江省健康医疗大数据政策： • 关于促进健康服务业发展的实施意见（2014.05.16，省政府）； • 关于促进健康信息服务业发展实施方案的通知（2014.12.19，省卫计委，省改委，省经信委） • 关于印发 2015 年全省卫生计生规划与信息化工作要点的通知（2015.04.08，省卫计委）； • 关于加快推进中医药健康服务发展的意见（2015.10.12，省政府办公厅）； • 关于加快推进中药产业传承发展的指导意见（2015.12.10，省政府）； • 关于印发浙江省“互联网＋”行动计划的通知（2016.01.14，省政府）； • 关于印发浙江省促进大数据发展实施计划的通知（2016.02.18，省政府）； • 关于印发浙江省医疗卫生服务体系规划（2016-2020 年）的通知（2016.05.16，省政府办公厅）； • 关于印发浙江省深化医药卫生体制改革综合试点方案的通知（2016.06.03，省政府）。

参考文献

[1] NUTBEAM D. The evolving concept of health literacy [J]. Social science & medicine, 2008, 67(12): 2072-2078.
[2] 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 国办发〔2016〕47 号 [EB/OL].(2016-06-30). http://www.moh.gov.cn/mohwsbwstjxxzx/s8555/201606/2a5b6612984e4c1daae45674a65adbde.shtml.
[3] WATSON. IBM Research: Watson [J]. Ibm Corporation.
[4] WATSONPATHS. IBM Research: WatsonPaths [J]. Ibm Corporation.
[5] 朱立峰，左铭，万歆，等. 医院临床研究中的大数据应用需求与策略 [J]. 中国数字医学, 2015, 10(12): 14-15.
[6] TOPOL E. The patient will see you now: the future of medicine is in your hands [M]. Basic Books, 2015.
[7] 袁琛. 医疗行业数据安全探析 [J]. 医学信息学杂志, 2016, 37(2): 43-46.
[8] 全国多省市数千万用户医保信息泄漏[EB/OL].(2014-12-31). http://bobao.360.cn/news/detail/1071.html.
[9] 中国互联网络信息中心（CNNIC）. 第 37 次中国互联网络发展状况统计报告 [EB/OL]. (2016-01-22). http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201601/t20160122_53271.htm.
[10] 智慧医疗与大数据 2015 年度报告 [J]. 信息化建设, 2016(2): 57-63.
[11] 许培海. 我国区域卫生信息平台建设现状及趋势研究 [J]. 中国数字医学, 2016, 11(5): 23-26.
[12] 浅谈医学大数据 [EB/OL][2015-03-25]. http://www.yuecang.com/wxgh_d748c5bef198/2822173.html.
[13] 邢帆. 医疗数据爆炸的获与惑 [J]. 中国信息化, 2015(2): 52-55.
[14] 大数据医疗：下一个产业“风口” [EB/OL]. (2015-10-19). http://www.thebigdata.cn/YingYongAnLi/15494.html.
[15] 孟小峰，张啸剑. 大数据隐私管理 [J]. 计算机研究与发展, 2015, 52(2): 265-281.
[16] 中华人民共和国网络安全法 [EB/OL]. (2016-11-08). http://www.miit.gov.cn/n1146295/n1146557/n1146614/c5345009/content.html.
[17] 个人信息权与隐私权有何区别 [EB/OL]. (2014-3-24). http://bjrb.bjd.com.cn/html/2014-03/24/content_163547.htm.
[18] 国家卫生计生委关于印发《人口健康信息管理办法（试行）》的通知 [EB/OL]. (2014-05-13) [2016-12-12]. http://www.nhfpc.gov.cn/guihuaxxs/s10741/201405/783ec8adebc6422bbebdf79db3868d0b.shtml.
[19] HIPAA for Professionals .
[20] Business Associate Contracts [EB/OL][2017-01-06]. https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html?language=es.
[21] 沈玲. 英国脱欧对数据保护立法的影响 [J]. 中国电信业, 2016(7): 52-53.
[22] https://ec.europa.eu/digital-single-market/en/news/directive-security-network-and-information-systems-nis-directive .
[23] 单寅. 欧美达成《隐私盾》协议引发的博弈思考 [N]. 人民邮电报, 2016.

感谢对OMAHA一直以来的支持与关注，并一如既往地期待您的意见和建议，让我们共同建设一个真正对推动民众获得个人健康医疗档案而努力的协作社区

关注个人健康医疗数据的开放，成为 OMAHA会员

OMAHA 热忱欢迎来自医疗和健康领域各个行业的个人和机构共同加入到医疗和健康数据开放的行列中来，通过协作的方式一同推进个人健康档案的落地。

OMAHA 对会员采取分类制管理，不同类型的会员享有的权益不同。OMAHA 提供三种会员等级以满足不同组织的需求：

- **赞助会员** (仅机构会员)：可直接与OMAHA秘书处联系；
- **正式会员** (机构会员和个人会员)：机构会员注册年费为5000元，个人会员注册年费为300元；
- **支持会员** (仅个人会员)：免费。

关于会员权益的具体信息请查看OMAHA官网网站、官方微信、宣传单页等。

通过官网申请会员

打开OMAHA官网（www.omaha.org.cn），
点击“会员申请”，填写信息并完成支付，
即可成为OMAHA会员

通过微信公众号申请会员

打扫描二维码，关注OMAHA微信，
点击下方“会员申请”，填写信息并
完成支付，即可成为OMAHA会员

关于 OMAHA

当今医疗服务已走到数据驱动的年代，不管是预防、诊断、检测，还是后期的治疗干预，医疗的本质就是信息处理。然而，医疗健康数据的碎片化格局已成为全球问题，个人无法获得完整的医疗健康数据，无法保证个人对优质医疗服务的高可及性和高质量性；同时，医生无法完成跨专科、跨地域的团队式医疗服务。

为了解决医疗健康领域数据分享这一共性问题，基于这一系列突出的未满足需求，行业内领先的相关机构和个人发起了开放医疗与健康联盟（Open Medical and Healthcare Alliance, OMAHA），目标促进数据的共享，抵抗数据的碎片化。

OMAHA目前已成立秘书处和五大工作组：

秘书处： 确定联盟的核心理念、宗旨和发展方向；制定联盟的管理机制和运作模式。优化联盟的内部管理，开展和组织与开放事业相关的各项工作和活动，并协调和配合各个工作组的事务。同时，建立联盟与外部生态之间的合作，构建有序的开放环境；

文化推广工作组： 促进个人医疗健康数据的可及性、完整性和可交换性，倡导相关医疗健康服务机构面向患者的数据开放；通过行业调研、文化宣教、医院开放度评价等活动，推动以个人为中心的医疗健康数据共享；

术语和数据工作组： 结合国内外已有标准以及行业应用现状，跟踪国内国际相关医疗健康标准组织，协作定义个人医疗健康相关术语与数据的标准，建立动态维护与更新机制，为开放文档格式工作组提供基础标准服务；

开放文档工作组： 整合碎片化的个人健康信息，充分借鉴欧洲Open EHR开源项目，协作制定开放个人健康档案格式，推动该文档格式在行业内的推广与应用；

隐私和安全工作组： 协作研究与制定个人健康数据在传输、交换过程中的身份认证、文档加解密等隐私与安全机制；跟踪国内外信息安全与隐私保护领域的法律法规，积极参与国内外相关标准的制定；

开源工作组： 支持医疗健康领域的开源（Open Source）活动，促进行业内医疗健康开源项目的交流、展示和应用，推动与其他工作组相关的基础共用件的开源化，重点支持开放个人健康档案编辑器（Open PHR Editor）开源项目；

进一步了解我们

网　　站：www.omaha.org.cn
微信公众号：china-omaha
联 系 电 话：0571-88937994
联 系 我 们：us@omaha.org.cn
加 入 我 们：hr@omaha.org.cn
地　　址：杭州市文三路90号东部软件园1号楼1122室