• 医学信息研究 •

国外医疗信息化领域隐私数据保护现状及其启示

王乐子 母健康 朱 翀 王思圆 弓孟春

（神州数码医疗科技股份有限公司 北京 100000）

〔摘要〕 详细阐述美国、欧盟及其部分成员国、加拿大、日本、新加坡、澳大利亚等国家和地区医疗信息隐私保护领域立法现状及相关法案特点，分析我国医疗隐私信息保护立法现状与不足，提出相应建议，为建立国内医疗数据隐私法案提供参考。

〔关键词〕 HIPAA；个人信息安全；医疗隐私数据

〔中图分类号〕R－056 〔文献标识码〕A 〔DOI〕10.3969/j.issn.1673－6036.2019.02.004

Status Quo and Enlightenment of Private Data Protection in Medical Informatization Domain Home and Abroad *WANG Lezi*, *MU Jiankang*, *ZHU Chong*, *WANG Siyuan*, *GONG Mengchun*, *Digital China Health Technologies Corporation*, *BeiJing 100000*, *China*

〔**Abstract**〕 The paper elaborates on the current legislative situation and features of relevant legislation concerning the protection of medical information privacy in countries and regions such as the U.S., the EU and some of its member states, Canada, Japan, Singapore, Australia, etc. It also analyzes the status quo and insufficiency of legislation on medical private information protection in China, according to which it makes suggestions for the references of domestic legislation on medical data privacy.

〔**Keywords**〕 HIPAA; personal information security; Medical privacy data

1 引言

从信息技术（Information Technology，IT）时代进入数据技术（Data Technology，DT）时代，各行各业经年积累的数据为行业发展提供丰厚的资源。依据不完全统计 2011 年美国产生 150EB 医疗相关数据，如保持目前的增速数据量很快会达到 ZB 和 YB 的级别。据统计部门估计到 2020 年医疗数据量将是 2009 年数据量的 44 倍。仅加州的一个医疗健康服务系统就拥有将近千万的会员和 44PB 左右的电子健康记录（Electronic Health Records，EHR）。

医疗卫生行业的数据量大且种类复杂，其中包含的价值也极为丰富。医疗数据的来源主要有 3 类：一是医学医药研究；二是医院临床应用，即诊断信息和临床操作；三是就医患者行为记录和社交网络。对这些数据进行保存、处理、分析研究可以帮助医护工作者做出更为精确的诊断和决策。个人健康数据已成为一种极为重要的资源，随着健康数据的快速增长，分析、分享个人健康数据如电子病历、临床检验、医疗影像数据等将成为提升病症早期的诊断率和智能化水平的关键[1]。这些有待发掘的资源随着大数据技术的发展必将成为未来数字化

〔收稿日期〕 2018－06－05

〔作者简介〕 王乐子，硕士；通讯作者：弓孟春，博士。

时代的重中之重，然而也随之面临严峻的问题，那就是个人医疗健康信息的安全问题。政府机构、医院、银行、企业和其他机构组织收集到的医疗数据中通常含有个人姓名、电话、邮箱、身份证号、居住地址、邮编等较为敏感的信息，如果这些信息不经处理就被公布会造成个人信息的泄露，影响个人信息安全。如何在不涉及个人敏感信息的情况下有效利用数据的潜在价值成为数据挖掘中的关键。据相关统计美国每年医疗费用财政拨款额度在5 万亿美元以上，通过利用医疗数据每年可以节省医疗开支3 000 ~4 500 亿美元。按此比例估算，面对我国每年2.4 万亿元的医疗投入，若能将医疗数据有效应用可节省医疗开支2 000 亿元左右，因此医疗数据的应用至关重要。

2 国外医疗信息隐私保护领域立法现状

2.1 美国

2.1.1 健康保险流通与责任法案（Health Insurance Portability and Accountability Act，HIPAA）概述 在1996 年美国克林顿总统任职期间签署并颁布的健康卫生领域的基本法[2]。HIPAA 的首要目的在于革新医疗领域，简化工作管理，降低成本费用，增强个人数据隐私保护。从实际意义来说，HIPAA 建立医疗领域的基本概念，明确实体的行为准则，规范具体的操作过程，标志着美国在医疗数据安全方面的法律达到领先水平。HIPAA 禁止未经患者本人授权的受保护的健康信息以任何形式进行交易或市场推广，规定受到约束的法律实体包括医疗健康提供方、保险提供方和数据清洗公司。由于绝大部分的医疗机构和保险公司都无法完全独立地完成所有业务，为增强隐私保护，HIPAA 也对第3 方商业合作伙伴进行约束。

2.1.2 HIPAA 的发展与完善 （1）发展。HIPAA 实施之初的目的在于保障员工在跳槽或失业后继续享受医疗健康保险。随着法案的不断发展，为提高美国医疗健康保险系统的效率和质量，HIPAA 着力推动对电子健康记录的采用。受保护的健康信息（Protected Health Information，PHI）包含较多可识别个人身份的医疗健康数据和其他相关数据，如保险单、账单消费信息、诊断医疗数据、临床医疗护理数据、影像数据等实验室结果和测试结果，所以 HIPAA 对这些个人健康信息的安全性和隐私性做出极其严格规定并建立完善的制度来界定和保护电子病历数据，防范数据泄露的相应风险。HIPAA 发布隐私和安全规则，主要目的在于保护个人医疗数据信息隐私的同时提高相关实体医疗的治疗水平和效率。此外由于医疗市场差异性很大，所以安全规则被设计的灵活又有可扩展性，使得相关实体可以根据组织规模、结构和相应风险实施恰当的策略、规章和技术。（2）完善。自 HIPAA 正式颁布后法案经历数次修正完善，使该法案对医疗信息隐私及安全保护更细致化和现代化[3-4]。2009 年 HIPAA 修改对于隐私数据安全的条目，增加对被管辖对象合作方的责任义务约束，以更好地保护个人数据安全。2009 年美国卫生及公共服务部（Department of Health and Human Service，HHS）引入美国复苏与再投资法案（American Recovery and Reinvestment Act，ARRA）和经济与临床健康信息技术法案（Health Information Technology for Economic and Clinic Health Act，HITECH），革新 HIPAA，此次革新是为了对个人信息的电子健康记录的使用，进一步强调 HIPAA 对个人隐私信息安全的重要性，也增加对泄露个人隐私数据行为的惩罚措施。革新后的法案于2010 年强制生效，作为 ARRA 的一部分，该法案获得400 亿美元刺激资金补贴用于鼓励其使用电子病历系统（Electronic Medical Record System，EMRS），与此同时 HITECH 还给该法案批准20 亿美元用于相关人才培训和基础建设[5]。2013 年初美国 HHS 颁布综合规则（Omnibus Rule），融合过去的 HITECH 和仅基因信息歧视法案（Generic Information Nondiscrimination Act，GINA），虽然 Omnibus Rule 是行政命令而不是法案，但其内容更加详细，对于违反规定的个人或者机构会受到更严重的处罚。

2.1.3 HIPAA 安全条例的基本标准 HIPAA 将数据安全的标准分为行政、技术和物理保障3 类，以建立更为完善的系统来保护信息系统的保密性、一致性和可用性以及患者的个人隐私。（1）行政保

障。建立和落实安全策略，研究并建设风险评估机制。该保障主要在于显示实体如何遵守安全规则的政策和程序，包括以下方面：安全管理流程、应急计划、指定安全责任、安全知识及意识培训、信息访问管理，认识和培训、评估、安全事故处理等。（2）物理保障。保护计算机系统运行环境和周围设备的安全。该保障主要在于对物理访问的控制，以防不适当的访问受保护的数据，包括以下方面：工作站的使用和安全、设备及媒体控制、设施出入控制。（3）技术保障。采用机器学习算法对数据进行主动防御保护，如数据分类、加密以及双向强身份认证等手段，采用现代信息存储方法，如磁盘阵列、数据备份、异地容灾等保证个人数据信息安全。该保障主要在于控制对计算机系统的访问和网络上传输的保护，包括以下方面：数据访问控制、审计控制以及数据完整性、个人或实体认证、传输安全。

2.2 欧盟及其部分成员国相关法案

2.2.1 欧盟 在 1995 年制订的数据保护指令（简称“95 指令”）是欧盟各国关于个人信息隐私保护的最低标准。随着数据爆发时代的来临，欧盟成员国的信息安全风险防控面临越来越多的挑战，为此欧盟委员会在“95 指令”和欧盟成员国现有相关信息保护法律基础上制定《通用数据保护条例》（General Data Protection Regulation，679/2016，GDPR）[6-7]。GDPR 的制订提高欧盟各成员国法律对个人数据保护的普适性与一致性。与各国现有的个人信息保护规定相比，GDPR 扩大数据主体权利，增加了数据控制者的义务，规范数据传输过程的程序。（1）数据主体权利。数据的被遗忘和删除权是 GDPR 较于其他安全条律的亮点，是保障个人医疗信息安全的重要手段，主要包括主体、客体以及不遵守规定的处罚措施。不论个体和企业是故意或者非故意违反，相关监管部门可以对其处以较高额的罚款，对违法行为起到震慑疏导作用。数据主体的同意必须是自愿、自由做出的并且是明确的。处理数据时，如果数据主体和控制者（非主体）之间地位存在不对等，主体的同意不能被作为使用数据的基础。当这种情况发生时要依据 GDPR 的规定进行处理[8-10]。GDPR 对个人隐私和特殊类别的数据做出专门规定，在处理这类数据时要先对其进行评估，最终结果会影响到处理数据的权限。关系到医疗的个人隐私数据都有其特定限制，不能被肆意处理。GDPR 的这些规定体现出对个人隐私的尊重和对个人数据安全的维护。（2）数据掌管者的义务。对非主体数据掌管者或处理者，如果该企业或机构处理数据时的人员超过一定数量，就要对其进行持续监控并任命数据保护专员以保护个人数据的安全。如果发生数据主体的信息被泄露的情况，GDPR 要求数据控制者于 24 小时内向数据安全部门报告相关泄露情况，以便采取补救措施，若是延误超过规定时间要解释超时原因。（3）个人数据传输规则。随着数据的迅述膨胀，个人数据在跨境的流量数据占有比例日益增大，此时个人信息就极易受到侵入。GDPR 规定对于个人数据的掌管者或处理者在处理个人数据时不论其在欧盟范围内是否设立机构，只要涉及欧盟内民众信息的采集、保存、传输等过程都必须受到 GDPR 的约束[11]。GDPR 会对无法保证数据传输安全的组织机构发出禁止令，以强制规范传输的安全形势。另外 GDPR 关于个人隐私数据在传输中制定的规则有助于信息在其间的安全流动。

2.2.2 部分成员国 （1）英国。2017 年英国女王批准相关“脱欧”法案，英国正式启动脱欧程序。2018 年 3 月 19 日欧盟与英国达成广泛过渡期条款协议，规定英国在 2020 年之前必须继续执行欧盟的所有规则，但没有未来决定中的话语权。英国拥有 210 年全国普查健康记录[12-13]，在遵循有效法律的情况下如此庞大的数据可以为临床医学研究、医药研发、公共卫生服务乃至全球医疗健康创造更多价值。英国凭借强大的数学和计算机领域实力，构建基于医疗数据应用系统平台的强大基础数据库，用来整理英国国民医疗服务系统数据并分类开放。关于医疗数据隐私问题，英国在 2005 年发布报告《生物医学研究与医疗卫生领域中数据的收集、连接和使用》[14-15]，建议政府机关或相关企业提高数据使用的透明度。2017 年英国发布《新的数据保护法案：计划的改革》声明，预计该法案将取

代《1998 年数据保护法》，使得数据的获取、迁移和删除权利更为严格。英国在隐私数据使用方面，除按照《数据保护法案》和《人权法案》外，主要通过征得数据主体同意和去识别使用数据匿名两种方法。在发布的新法案中扩充个人数据信息范围，任何可能泄露个人行踪的数据信息被列为要保护的信息；法案也增加被遗忘权，即社交网络媒体所据有的个人学生时代的数据信息，个人有权要求相关数据实体和控制者将其删除。与此同时，若是违反法案条例将面临极为严厉的手段制裁。（2）法国。作为欧盟成员，法国自 18 世纪大革命及《人权宣言》出台至今保护公民自身权利及其隐私权成为法国宪法的基本原则。20 世纪 70 年代末法国颁布的《法国自由、档案、信息法》是关于公民信息安全的法律，于 1983 年又颁布《在个人性质数据自动处理方面保护个人的公约》，这些法律均详细规定法国对于公民隐私数据进行保护的具体措施，为个人隐私数据安全提供保证。由于在医疗领域对于个人信息数据的使用在信息安全法中没有给出特别的规定和限制，所以法国政府设立独立的部门，专门对申请使用个人数据信息的人员或部门进行处理，以确保个人信息的安全使用。此外 2013 年在巴黎召开的大数据大会上法国政府宣布未来 5 年将在教育、医疗健康等重点项目投入 1 150 万欧元，用于拓展法国的大数据领域。

2.3 加拿大

加拿大政府注重个人信息隐私以及信息的透明度和人民的知情权，为保证民众知情权建立《信息获取法》，为保护公民个人隐私颁布《隐私法》和《个人信息保护与电子文件法》（Personal Information and Protection and Electromic Documents Act，PIPEDA），其中《隐私法》规定政府组织机构在收集、储存、调用公民信息时要确保信息的安全，同时赋予公民更正个人隐私数据信息的权利。2001 开始实施的 PIPEDA 规定私营企业和机构对于处理个人信息的原则。为更大限度地保护个人信息，加拿大联邦政府专门设立个人隐私信息保护机构，并且将国际事务活动、国家防务调查普查以及执行法律行为得到的个人信息称为“豁免信息库”，有效地淡化公民的隐私，也体现利益制衡的原则。《隐私法》说明加拿大政府对于公民隐私数据信息的保护不是无条件的，公民的隐私信息只有在符合国家利益的情况下才会被保护，另外如果个人信息和公共利益发生冲突时，加拿大政府法律规定要优先保护公共利益。加拿大制定的政府法律和个人隐私数据之间的制衡可以为我国在隐私数据保护层面提供借鉴。

2.4 日本

日本有关个人隐私数据信息保护的法律法规在 2003 年以前主要适用在政府机构和计算机行业涉及到个人信息时。当时日本政府对非政府组织机构在涉及个人信息保护问题上没有相应法律，各种私营企业、电商、金融机构、保险公司等拥有的客户信息较多，在没有法律规范的情况下出现个人隐私数据被非法买卖、被披露等泄露行为，也不能得到有震慑效果的处罚。所以限制私营企业对个人隐私数据的利用成为必然，2003 年日本颁布《个人信息保护法》[16]，该法律是在有效利用个人数据信息的情况下对公民数据信息进行保护，以保证公民的合法权利不受侵害，从效用来讲该法可以称为企业机构规范法，其面向的对象是具有个人数据信息的企业和组织机构，受到相关行政机构的督察和管理。2013 年安倍政府发布关于未来开放公共数据和大数据为核心的战略布局宣言。2014 年增加宣言内容，即鼓励在医疗大数据平台下灵活有效地利用医疗相关数据来改善现有的医疗环境、加强疾病的防控能力。宣言增加的内容一是建立多种主题的医疗服务机构，以提高医疗服务的效率；二是医疗数据和网络相结合，对于医院、保险公司等企业单位提供的数据进行分析利用，达到降低医疗费用的效果；三是健全政府制度，设立首席信息技术长官，用于监督日本信息数据的安全和利用情况。

2.5 新加坡

为限制个人数据信息被非法用于商业或非法欺诈活动，近期新加坡个人数据信息保护相关部门修订《个人数据保护法案》（Personal Data Protection

Act，PDPA），主要为限制一些企业和机构使用公民身份证的权利范围。另外新加坡政府还公布用于保护政府有关部门隐私数据共享的法案。PDPA 为企业机构在使用公民隐私信息方面提供模式化管理，使其虽然拥有隐私数据却不能随便使用。如不能将身份证用于创建零售账户，但是可以用来查询医疗患者。由于一些公司或者企业获取公民电话号或身份证号的方式极多，所以对其使用方式及目的加以规范和引导。

2.6 澳大利亚

在关于个人信息安全的保护方面一直都是世界的先行者，20 世纪 80 年代就已制订《隐私法》，专门用于保护个人数据信息安全。随着网络的发展，澳大利亚政府在网络安全方面有很强的警觉性，2009 年制订《国家信息安全战略》，随着对法案的不断补充和改进，目前澳大利亚政府的数据信息保护极为完善，如网络硬件基础设施、个人隐私数据的电子记录、数据传输以及政府信息保护方面都形成稳定的保护规则。

3 各国安全法案对中国的启示

3.1 中国医疗隐私信息保护立法现状与不足

中国目前尚未出台专门的个人信息保护法，相关规定散见于多部法律法规和规章制度中。2017 年 6 月 1 日起正式施行的《中华人民共和国网络安全法》中明确规定，网络运营者不得泄露、篡改、毁损其收集的个人信息；除经过处理无法识别特定个人且不能复原的信息外，未经被收集者同意不得向他人提供个人信息，但是该法律中没有明确规定处理手段和方法。由中华人民共和国国家质量监督检验检疫总局和中国国家标准化管理委员会于 2017 年 12 月 29 日发布，2018 年 5 月 1 日起实施的《信息安全技术 个人信息安全规范》[17-18]对个人数据的收集、存储、应用、传输各个环节提出十分确切具体的规定。该规范为推荐性的国家标准且没有专门针对医疗行业的条款，几乎将所有与医疗行为相关而产生的数据都定义为个人敏感数据，强调收集个人敏感信息时的明示同意，又将几项与医疗行业相关情况的条款列为征得授权同意的例外情况中。包括个人隐私数据控制者是国家研究机构，出于社会利益对个人隐私数据进行统计和研究，但是在对外宣布研究结果时必须对个人隐私数据进行去标识化处理的；与公共安全、公共卫生、重大公共利益直接相关的；为维护他人生命财产合法权益但又很难得到信息主体本人同意的。2017 年 8 月 15 日由中国标准化委员会发布《信息安全技术 个人信息去标识化指南》，该文件目前还是征求意见稿，主要内容为去标识化的方法论，描述个人信息去标识化的目标和原则，提出去标识化过程和管理措施。去标识化的定义是通过特定算法或方法处理个人隐私数据信息，经过处理后的数据信息在不借助其他技术或信息的情况下无法反向识别信息的主体。中国目前没有专门针对医疗信息及个人健康隐私保护的法规、标准，对医疗信息中的敏感部分没有统一的界定标准，对于相关信息的去标识化及其效果也没有定量的标准去评估。各国关于个人隐私保护方面都有相应的立法，这些法案的侧重点不完全相同，尤其是美国的 HIPAA，它是专门针对医疗信息与个人隐私的法案，将信息安全保护与医疗健康领域紧密结合，具体规范敏感信息的保护要求和标准。对各个国家的相关法案进行整体性的研究会对中国未来相关标准的制定给予一定的启示和帮助[19-22]。

3.2 对国内的策略和建议

3.2.1 患者隐私信息泄露途径分析 （1）非交互式泄露。不论是在欧美发达国家还是在我国，医疗机构、保险公司以及医护人员均有保护就医者隐私的法定义务。但医疗机构内部管理存在一定的漏洞，有可能导致患者隐私数据泄露。然而在法律中却没有规定对擅自泄露隐私数据的行为采取何种惩罚手段。随着数据的日益增长，此方面的立法日趋迫切。（2）交互式泄露。医生或医疗机构相关学者为进行临床研究会从医院或其他医疗机构拿到患者的隐私数据进行分析；另外我国正致力于建立电子病历，以实现局部或全国医疗信息共享。虽然这两种情况是以便民为目的，也属于征得授权同意的例

外情况，但也面临隐私数据泄露的问题。医疗领域的研究人员往往对于去标识化的相关知识比较欠缺，在缺少硬性指导的情况下，一般研究人员仅能根据自身常规手段对于一些直接标识符进行处理。需要注意的是经过常规手段进行去标识化后的个人数据也不能完全确定是安全的。随着数据挖掘、机器学习、人工智能等技术的应用和发展，大数据分析能力越来越强大，而海量的数据本身就蕴藏着价值，尤其是医疗行业，目前医疗大数据正向着多源联合分析的方向发展。其数据内容不仅包含常规的临床数据，从数据来源来讲还包含医疗从业者提供的电子医疗档案、健康档案、临床测试结果、临床评估记录；来自于患者社交网络的行为数据以及患者提供的结果研究数据；医药企业提供的市场营销、医疗、研发数据；医保机构持有的报销数据等等。而在对大数据中多源数据进行综合分析时，分析人员更容易通过关联分析挖掘出更多的个人信息，从而进一步加剧个人信息泄露的风险[23]。在大数据时代，对个人数据进行安全保护既要注意防止因数据丢失而直接导致的个人信息泄露，也要注意防止因挖掘分析而间接导致的个人信息泄露，这种综合保护需求带来的安全挑战十分艰巨。

3.2.2 建议 （1）完善个人隐私法律法规。公立医院改革是我国医药卫生领域改革的重点，然而医疗数据的信息化是改革的有效手段。要体现信息化的有效性就应对电子病历进行立法，确保其有效性、安全性，规范相关实体的权利和义务以及侵犯个人隐私数据所要承担的法律后果，提高法案的可实施性。另外应制定医疗健康信息大数据安全标准，包括数据的采集、储存和传递方式等，以保证医疗机构和企业之间数据的规范性、安全性、共享性以及流通性。（2）发展保护个人数据隐私技术。个人数据的隐私问题离不开信息技术的支持。随着信息技术的快速发展和应用，一些新问题、新情况也会出现，所以隐私技术要跟上信息技术的发展。可通过建立医疗领域的数字身份、数据限制访问信息系统、升级加密手段等加强对隐私数据的防护。如在信息去标识化方面，相关加密算法可以考虑使用循环神经网络（Recurrent Neural Network，RNN）、长短期记忆网络（Long Short Term Memory，LSTM）、分段卷积神经网络、分段递归神经网络等。同时还应加强去标识化和再识别风险相关算法研究，在数据共享前针对已去标识化的数据计算数据再识别风险，以确保共享数据安全。也可以采用其他手段进行研究的内部数据共享，如加密等方法。总之，在敏感信息处理方面，要跟上信息技术的发展，以确保医疗健康数据安全。（3）加强医疗数据信息管理。虽然我国目前正在推动医疗领域的信息披露工作，但是对个人数据的使用和披露没有确切的规定，也没有完善的数据信息保护机制。我国应加强医疗隐私数据的安全风险评估和保护。可以根据HIPAA 建立医疗隐私数据安全管理机构，包括医疗数据管理委员会、隐私数据业务和技术部门以及安全风险评估部门；完善相关政策，培训数据安全专业人才。而相关企业要定期组织员工进行信息安全培训指导，增强安全意识，做好安全评估，预防可能出现的风险。另外我国应将个人信息的保护和披露有效结合起来，尽量做到医疗数据的质量和信息保护的平衡。在使用研究数据的基础上要对发布的信息进行有效界定和处理，避免个人数据的泄露。

4 结语

总体来说，虽然我国对于个人数据保护及相关基本原则进行规定，但是现阶段没有建立起完整的个人信息隐私安全立法系统，涉及隐私安全的规定分散于法律、行政规范中，并且内容冗杂，缺乏层次性、针对性和统一性，使得医疗大数据在我国的应用一直停滞不前[24-29]。另外目前的规定主要是针对数据使用的正当和必要程序等方面，对于不同类别的个人数据其保护水平和要求的细分程度不足，使用规范也应进一步细化。可参照国外相关法律内容，在涉及医疗数据隐私保护方面需要对更大范围的数据保护立法进行补充和优化。

参考文献

1 Costa F F. Big Data in Biomedicine [J]. Drug Discover Today, 2014, 19 (4): 433-440.

2 Act A. Health Insurance Portability and Accountability Act of 1996 [J]. Public Law, 1996 (104): 191.

3 Baumer D, Earp J B, Payton F C. Privacy of Medical Records: IT implications of HIPAA [J]. ACM SIGCAS Computers and Society, 2000, 30 (4): 40 - 47.

4 Annas G J. HIPAA Regulations - a new era of medical - record privacy?[J]. New England Journal of Medicine, 2003, 348 (15): 1486 - 1490.

5 US Department of Health and Human Services. Summary of the HIPAA Privacy Rule [M]. Washington DC: Author, 2003.

6 Raghupathi W, Raghupathi V. Big Data Analytics in Healthcare: Promise and Potential [J]. Health Information Science and Systems, 2014, 2 (1): 3.

7 Zhang Y, Guo SL, Han LN, et al. Application and Exploration of Big Data Mining in Clinical Medicine [J]. Chinese Medical Journal, 2016, 129 (6): 731 - 738.

8 Voss W G. Looking at European Union Data Protection Law Reform Through a Different Prism: the proposed EU general data protection regulation two years later [J]. Social Science Electronic Publishing, 2015, 17 (1): 12 - 24.

9 Belle A, Tiagarajan R, Soroushmehr S M, et al. Big Data Analytics in Healthcare [J]. Biomed Res Int, 2015, 54 (6): 546.

10 Pearce H. Big Data and Reform of the European Data Protection Framework: an overview of potential Concerens associated with proposals for risk management - based appraches to the concept of personal data [J]. Information & Communications Technology Law, 2017, 26 (3): 1 - 24.

11 Lusoli W, Bacigalupo M, Lupiáñezvillanueva F, et al. Pan - European Survey of Practices, Attitudes and Policy Preferences as Regards Personal Identity Data Management [J]. Social Science Electronic Publishing, 2012, 19 (6): 95 - 123.

12 Hood L, Flores M. A Personal View on Systems Medicine and the Emergence of Proactive P4 Medicine: predictive, preventive, personalized and participatory [J]. New Biotechnology, 2012, 29 (6): 613 - 624.

13 Victor J M. The EU General Data Proection Regulation: toward a property regime for protecting data privacy [J]. Social Electronic Publishing, 2013, 123 (2): 513 - 528.

14 Crump C, Sundquist K, Winkleby M A. Transnational Research Partnerships: leveraging big data to enhance US health [J]. Journal of Epidemiology & Community Health, 2015, 69 (11): 1029 - 1030.

15 Benson T. Principles of Health Interoperability HL7 and SNOMED [M]. London: Springer, 2010.

16 Kwon H. Transforming the Developmental Welfare State in East Asia [J]. Development and Change, 2005, 36 (3): 477 - 497.

17 中华人民共和国全国人民代表大会常务委员会. 中华人民共和国网络安全法 [S]. 2016 - 11 - 07.

18 颜延, 秦兴彬. 医疗健康大数据研究综述 [J]. 科研信息化技术与应用, 2014, 5 (6): 3 - 16.

19 McGraw D. Building Public Trust in Uses of Health Insurance Portability and Accountability Act De - identified Data [J]. Journal of the American Medical Informatics Association, 2013, 20 (1): 29 - 34.

20 Hanf M, Quantin C, Farrington P, et al. Validation of the French National Health Insurance Information System as a Tool in Vaccine Safety Assessment: application to febrile convulsions after pediatric measles/mumps/rubella immunization [J]. Vaccine, 2013, 31 (49): 5856 - 5862.

21 Bishop S K, Winckler S C. Implementing HIPAA Privacy Regulations in Pharmacy Practice [J]. Journal of the American Pharmaceutical Association, 2002, 42 (6): 836 - 846.

22 Zhang R, Liu L. Security Models and Requirements for Healthcare Application Clouds [C]. Florida: IEEE, International Conference on Cloud Computing, 2010: 268 - 275.

23 Appari A, Johnson M E. Information Security and Privacy in Healthcare: current state of research [J]. International Journal of Internet and Enterprise Management, 2010, 6 (4): 279 - 314.

24 AlShwaier A A, Emam A Z, Arabia - Riyadh S. Data Privacy on E - Health Care System [J]. International Journal of Engineering, Business and Enterprise Applications, 2013, 3 (2): 89 - 99.

25 Xhafa F, Feng J, Zhang Y, et al. Privacy - aware Attribute - based PHR Sharing with User Accountability in Cloud Computing [J]. Journal of Supercomputing, 2015, 71 (5): 1607 - 1619.

26 汤啸天. 个人健康医疗信息和隐私权保护 [J]. 同济大学学报: 社会科学版, 2006, 17 (3): 117 - 123.

27 Hersh W R. Adding Value to the Electronic Health Record Through Secondary use of Data for Quality Assurance, Research, and Surveillance [J]. Clin Pharmacol Ther, 2007, (81): 126 - 128.

28 HIPAA 法 [EB/OL]. [2017 - 04 - 10]. http://hipaa.wisc.edu/ResearchGuide/Deidentifi - cation.html.

29 Chan K S, Fowles J B, Weiner J P. Electronic Health Records and the Reliability and Validity of Quality Measures: a review of the literature [J]. Medical Care Research and Review, 2010, 67 (5): 503 - 527.